A Unified Wormhole Attack Detection Framework for Mobile Ad hoc Networks

Thesis

A UNIFIED WORMHOLE ATTACK DETECTION FRAMEWORK FOR MOBILE AD HOC NETWORKS

Jonny Karlsson

A thesis submitted in partial fulfilment of

the requirements for the degree of Doctor of Philosophy

Department of Computing and Communications

Faculty of Mathematics, Computing & Technology
The Open University
Milton Keynes

December 2015

ABSTRACT

The Internet is experiencing an evolution towards a ubiquitous network paradigm, via the so-called *internet-of-things* (IoT), where small wireless computing devices like sensors and actuators are integrated into daily activities. Simultaneously, infrastructure-less systems such as *mobile ad hoc networks* (MANET) are gaining popularity since they provide the possibility for devices in *wireless sensor networks* or *vehicular ad hoc networks* to share measured and monitored information without having to be connected to a base station. While MANETs offer many advantages, including self-configurability and application in rural areas which lack network infrastructure, they also present major challenges especially in regard to routing security. In a highly dynamic MANET, where nodes arbitrarily join and leave the network, it is difficult to ensure that nodes are trustworthy for multi-hop routing. Wormhole attacks belong to most severe routing threats because they are able to disrupt a major part of the network traffic, while concomitantly being extremely difficult to detect.

This thesis presents a new unified wormhole attack detection framework which is effective for all known wormhole types, alongside incurring low false positive rates, network loads and computational time, for a variety of diverse MANET scenarios. The framework makes three original technical contributions: *i)* a new accurate wormhole detection algorithm based on *packet traversal time and hop count analysis* (TTHCA) which identifies infected routes, *ii)* an enhanced, dynamic *traversal time per hop analysis* (TTpHA) detection model which is adaptable to node radio range fluctuations, and *iii)* a method for automatically detecting time measurement tampering in both TTHCA and TTpHA.

The thesis findings indicate that this new wormhole detection framework provides significant performance improvements compared to other existing solutions by accurately, efficiently and robustly detecting all wormhole variants under a wide range of network conditions.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my principal supervisor from the Open University Prof. Laurence S. Dooley and my "external" supervisor Dr. Göran Pulkkis from Arcada University of Applied Sciences in Helsinki. This thesis would not have been accomplished without their constructive feedback on both scientific writing and technical issues as well as their continuous and strong support, expertise and guidance throughout the whole process. A more helpful and supportive supervision team is very difficult to find. I would also like to thank my second supervisor Dr. David Chapman from the Open University for his help in the early stages of my doctoral studies and for providing valuable feedback on the final version of my thesis.

I am greatly indebted to my employer Arcada for the opportunity to carry out my doctoral studies. I also want to thank Arcada's internal fund "Studentstipendifonderna vid Arcada" for the crucial financial support. Without the flexibility and cooperation from my co-workers it would have been impossible to go through the whole study process within a reasonable timeline. I am delighted to be surrounded with very good friends among the Arcada personnel who have supported and encouraged my research in many ways.

I wish to thank all staff members as well as former and current students of the *next generation multimedia technologies* (XGMT) research group at The Open University. You have given me valuable help and advices throughout my studies, created a friendly research environment and have always made my visits to the Open University campus extremely enjoyable. Many thanks also to all of you who sacrificed your own research time in proof-reading my thesis.

I am deeply grateful to my close relatives including my father, brother and my parents-in-law for all support, encouragement and help with looking after my children during the busy stages of the PhD project. Last but not least, I would like to warmly thank my lovely wife

Sonja for the sacrifices you have made as well as the understanding, flexibility and love you have shown during this long process. My adorable children, Ella, Kasper and Ruben, thank you for all the positive energy you have shared and for helping me to focus also on other things than research.

DECLARATION

The work presented in this thesis is an original contribution of the author. Parts of the thesis have appeared in the following:

Peer-Reviewed Publications:

Karlsson, J., Dooley, L.S. & Pulkkis, G. (2011) 'A New MANET Wormhole Detection Algorithm based on Traversal Time and Hop Count Analysis", Sensors, vol. 11, no. 12, pp. 11122-11140.

Karlsson, J., Dooley, S., Laurence & Pulkkis, G. (2012) 'Routing Security in Mobile Ad hoc Networks', Issues in Informing Science and Information Technology, vol. 9, pp. 369-383.

Karlsson, J., Dooley, L.S. & Pulkkis, G. (2013) 'Identifying Time Measurement Tampering in the Traversal Time and Hop Count Analysis (TTHCA) Wormhole Detection Algorithm', Sensors, vol. 13, no. 5, pp. 6651-6668.

Karlsson J., Dooley L.S. and Pulkkis, G. (2016) 'A Packet Traversal Time per Hop based Adaptive Wormhole Detection Algorithm for MANETs', Proceedings of the 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM'16). Split, Croatia, 22-24 September. IEEE, pp. 1–7. **Winner of Best Paper Award.**

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ΔTVE	ΔT Vector Extension
4G	Fourth Generation
5G	Fifth Generation
AODV	Ad hoc On-demand Distance Vector
ARAN	Authenticated Routing for Ad hoc Networks
ARF	Alternate Route Finder
BAIDS	Biologically Inspired Artificial Intrusion Detection System
CONFIDANT	Cooperation of Nodes' Fairness in Dynamic Ad hoc NeTworks
CORE	Collaborative Reputation
CWS	Congestion Windows Surveillance
DelPHI	Delay Per Hop Indicator
DoS	Denial-of-Service
DPH	Delay Per Hop
DR	Data Rating
DSDV	Destination-sequenced Distance Vector
DSR	Dynamic Source Routing
FACES	Friend-based Ad hoc Routing using Challenges to Establish Security
FEEPVR	First End-to-End Protocol with Variable Ranges
FP	False Positive
FR	Friend Rating
FrAODV	Friendship-based AODV
GPS	Global Positioning System
HC	Hop Count
HM	Hidden Mode

I-B	In-Band
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
LMT	Local Most Trustable
LOS	Line-of-Sight
LS	Local Supervision
MAC	Medium Access Control
MAC	Message Authentication Code
MANET	Mobile Ad hoc Network
MDS-VOW	Multi-Dimensional Scaling Visualisation of Wormhole
MHA	Multi Hop Count Analysis
MITM	Man-in-the-Middle
M-TTM	Modified TTM
NIA	Node Isolation Algorithm
NPA	Neighbour Probe Acknowledge
NR	Net Rating
ns	Network Simulator
ns-2	Network Simulator version 2
O-B	Out-of-Band
OLSR	Optimized Link State Routing
OS	Operating System
PD	Propagation Delay
PM	Participation Mode
PP	Projection Pursuit
PTT	Packet Traversal Time
QoS	Quality of Service

RERR	Route Error
RREP	Route Reply
RREQ	Route Request
RSSI	Received Signal Strength Indicator
RTT	Round Trip Time
RWM	Random Waypoint Mobility
SA	Security Association
SAM	Statistical Analysis of Multipath
SAODV	Secure AODV
SAR	Security Aware Ad hoc Routing
SCREWED	Secure Channel Reciprocity-based Wormhole Detection
SEAD	Secure Efficient Ad hoc Distance Vector
SEEEP	Simple and Efficient End-to-end Protocol
SLSP	Secure Link State Routing Protocol
SRAC	Secure Routing Against Collusion
SRP	Secure Routing Protocol
SWAN	Statistical Wormhole Apprehension using Neighbours
TAODV	Trusted AODV
TESLA	Timed Efficient Stream Loss Tolerant Authentication
TF	Threshold for Friendship
THL	Traversed Hop List
TIK	TESLA Instant Key disclosure
TR	Timestamp Resolution
TSR	Two-level Secure Re-routing
TTHCA	Traversal Time and Hop Count Analysis
TTM	Transmission Time based Mechanism
TTpHA	Traversal Time per Hop Analysis

VANET	Vehicular Ad hoc Network
WAD-HLA	Wormhole Attack Detection using Hop Latency and Adjoining node analysis
WAP	Wormhole Attack Prevention
WARP	Wormhole Avoidance Routing Protocol
WPT	Wormhole Prevention Timer
WSN	Wireless Sensor Network
ZRP	Zone Routing Protocol

LIST OF VARIABLES

$\{\Delta T_{TOT}\}_i$	ΔT_{TOT} as calculated at node i
ΔT_F	Artificial packet processing time measurement value to be added to ΔT_{TOT}
ΔT_{F1}	ΔT_F - ΔT_{F2}
ΔT_{F2}	ΔT_F - ΔT_{F1}
ΔT_i	The sum of RREQ and RREP packet processing delays at node i
$\{\Delta T_{RREP}\}_i$	RREP packet processing time at node i
$\{\Delta T_{RREP\_TTHCA}\}_i$	$\text{RREP}_{\text{TTHCA}}$ packet processing time at node i
$\{\Delta T_{RREQ}\}_i$	RREQ packet processing time at node i
ΔT_{TOT}	The sum of all ΔT_i on a route
ΔT_{wh}	The sum of all ΔT_i at the legitimate nodes through which I-B wormhole nodes tunnel routing packets
ρ	Node traffic load
ρ_{max}	Maximum node traffic load
D_C	Number of correctly detected infected routes
D_F	Number of falsely detected routes
D_{MAX}	Maximum packet travel distance
DPH_I	Delay per hop for route I
E_{TR}	The measurement error due to the TR for a recorded timestamp
HC_I	HC fore route I
HC_i	HC from node i to the destination node
L	Network length
N	Number of MANET nodes
N_{HR}	Number of healthy route samples
N_{IR}	Number of infected route samples

N_{MIN}	Minimum size of vector V
PD_{MAX}	Maximum PD
PD_{RREP}	PD of a RREP packet tunnelled between two wormhole endpoints
PD_{RREQ}	PD of a RREQ packet tunnelled between two wormhole endpoints
PTT_F	An artificial value to be added to $PTT_{i,i+1}$
PTT_i	Measured PTT between node i and the destination node
$PTT_{i,i+1}$	Measured PTT between node i and $i+1$
Q_C	Critical value for a chosen confidence level α used in Dixons's Q-test
R	Maximum node radio range
R_i	Maximum momentary radio range for node i
$r_{i,i+1}$	The distance between two successive nodes on a route path
$RREP_{lim}$	RREP number limit
RTT_i	Measured RTT between node i and the destination node
RTT_I	RTT for route I
$RTT_{i,i+1}$	Measured RTT between node i and $i+1$
RTT_{wh}	RTT of the wormhole link
r_{wh}	Length of wormhole link
S	Packet propagation speed
T	Maximum permissible difference between two adjacent DPH_I values
T_A	Actual time of incoming/outgoing routing packet
T_C	The time when a hardware clock checks for an event
t_{exp}	Packet expiration time
t_{loc1}	Local packet transmission time

t_{loc2}	Local packet reception time
$\{T_{RREPr}\}_i$	Timestamp recorded at node i when receiving the first bit of a RREP
$\{T_{RREPs}\}_i$	Timestamp recorded at node i when sending the first bit of a RREQ
$\{T_{RREQr}\}_i$	Timestamp recorded at node i when receiving the first bit of a RREQ
$\{T_{RREQs}\}_i$	Timestamp recorded at node i when sending the first bit of a RREQ
T_S	Packet service time
t_{wh}	The delay of a wormhole link
V	Vector of $PTT_{i,i+1}$ values
W	Network width
x	The smallest permissible $r_{i,i+1}$ in relation to r_{wh}
α	Confidence level for Dixons's Q-test
θ	The maximum permissible $PTT_{i,i+1}$
σ_R	Relative standard deviation

1. INTRODUCTION

The Internet is experiencing an evolution from the traditional desktop to a ubiquitous paradigm where a multitude of small computing devices, such as computer chips, actuators, and small sensors are involved in daily activities and routines. These devices can collect, store and process information which will be shared with other devices and collaborate in creating smart environments and systems (Mashal et al., 2015). This fast emerging global and collaborative network structure is popularly known as the *internet-of-things* (IoT) (Li et al., 2014).

The IoT trend is leading to an ever increasing number of devices being connected to the Internet and the evolving of new more effective types of wireless infrastructures, such as *fourth* and *fifth generation* (4G and 5G) network technologies. Simultaneously, infrastructure-less and self-configuring systems like *mobile ad hoc networks* (MANET) have also gained popularity among the research community. The MANET paradigm provides the possibility for example, for *wireless sensor networks* (WSN) and *vehicular ad hoc networks* (VANET) to be able to share measurements and monitor information without being connected to a base station. These are therefore widely recognized technologies e.g. for several IoT application domains in smart cities (Bellavista et al., 2013; Yovanof & Hazapis, 2009).

While self-configuring, infrastructure-less and dynamic topological features bring significant advantages including easier and faster large-scale deployments, at the same time they also generate considerable challenges in regard to for example, the *quality of service* (QoS) provisioning (Marwaha, et al., 2008), connectivity management (Dengiz, et al., 2011), end-to-end delay and packet loss on multi-hop routes in latency-sensitive applications (Lindeberg, et al. 2011) and *internet protocol* (IP) address management (Choudhury et al.,

2015). Security is recognized as one of the most significant challenges to facilitate wide scale MANET adoption. An overview of MANETs and their main security challenges now follows.

1.1. Overview of Mobile Ad hoc Networks and their Security Challenges

A MANET device can move independently in any direction, at any time. Therefore such networks have a dynamic topology. MANETs can be utilized for a variety of applications including military communications and rescue operations where a network infrastructure either does not exist or has been eliminated. They can also be seen as an alternative to Internet connectivity, for devices in both rural and urban areas which are temporarily located out of range of an Internet access point (Ding, 2008). Several communication network paradigms including WSN, VANET, wireless mesh, opportunistic and people-centric networks are examples of real-world applications based on the MANET paradigm (Conti & Giordano, 2014).

General purpose MANETs have been an intensive research area for decades but have not yet significantly impacted upon the wireless networking market mainly due to several weaknesses in design and research approach (Basagni et al., 2013). Security is one of the key challenges since the infrastructure-less nature of MANETs leads to many new threats compared to wired and wireless infrastructure networks. These threats include (Goyal et al., 2010):

- Lack of centralized management makes network monitoring and security attack detection a challenging task.
- MANETs have high scalability which sets a correspondingly high requirement on the security protocols. Security mechanisms must be capable of handling both small and large networks.

- In dynamic network topologies, trusted relations between nodes are intrinsically difficult to implement.
- Limited power supply leads many nodes to behave in a selfish manner which can disrupt the routing.
- MANET routing algorithms generally rely on all network nodes being non-malicious and cooperative which makes it relatively easy for a malicious node to disrupt routing.

Routing is an essential feature of any computer network to enable communications over multiple hops. MANETs, particularly WSNs, typically consist of energy-scarce, hardware-restricted devices with short communication ranges and thus successful information sharing in such networks is highly dependent on multi-hop communications. If routing is disrupted, it means that data packets are dropped and they cannot reach their destination. MANET routing is particularly vulnerable from a security point of view since there are no dedicated routers and each node in the network must take part in the routing process. Thus, routing can easily be disrupted, for example by selfish nodes for battery saving purposes or by nodes with malicious intentions. In the next section, an overview of the most well-known attacks on MANET routing is provided together with existing countermeasures.

1.1.1. Overview of Mobile Ad hoc Network Routing Security

Security threats on MANET routing can roughly be divided in two main types; *passive* and *active* attacks. A passive attack typically involves traffic monitoring with the intention to confiscate vital information from data packets, though the normal functionality of the network is not affected. Through a passive attack, a malicious node often tries to identify communication parties and functionality that potentially provides information to launch further attacks. In contrast, an active attack is performed with the intention to specifically

change the routing functionality. Examples of such attacks include (Karlsson, et al., 2012; Soni et al., 2010):

- Malicious modification of routing packets, e.g. falsely decreasing the *hop count* (HC) parameter of a routing packet such as in the *blackhole attack*, with the intention to advertise a short route and thus attract network communications.
- Spoofing an IP address for example, to capture data packets meant for other nodes.
- Fabrication, with the main purpose to drain off limited resources in other MANET nodes like battery power and network bandwidth.
- Selfish behaviour of a node which refuses to take part in the routing process for energy saving purposes.
- Wormholes, which are usually launched by two malicious nodes located far apart, who capture and tunnel routing packets to each other. As a result they attract a large portion of network traffic and create the illusion that the two wormhole endpoints are neighbours, even though there is a long distance between them.

A wormhole attack is a particularly severe threat on MANET routing since it is relatively easy to launch, difficult to detect and can cause major network communications disruption (Khabbazian et al., 2009; Hu et al., 2003). If a wormhole is successfully established in a MANET, the malicious wormhole nodes can choose to launch further attacks such as selectively dropping packets to disrupt network communication or capture confidential information by sniffing data packets. An example of a wormhole attack is visualised in Figure 1.1, where A is the source node, D is the destination node, M_1 and M_2 are malicious wormhole nodes and all the other numbered nodes are legitimate. In this scenario, the shortest route in terms of hops, will traverse intermediate nodes #2, #3, #4, #5 and #6. However, if M_1 records routing packets received from its neighbours, tunnels them to M_2 which in turn replays the tunnelled routing packets to its neighbours, then M_1 and M_2 create the illusion that the shortest route traverses the two wormhole nodes.

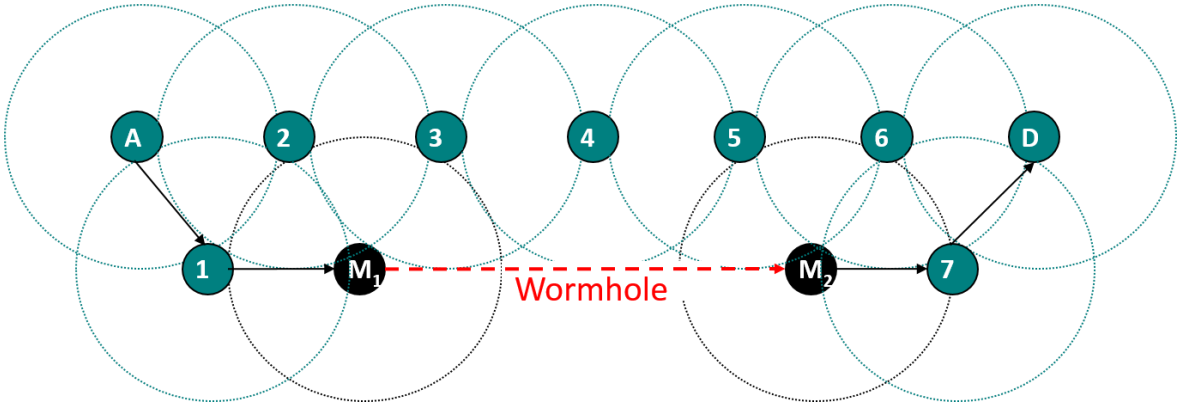

Figure 1.1: A wormhole attack example.

Wormhole attacks are difficult to detect mainly because they can be launched in several different modes where each mode sets its own requirements upon the detection algorithm:

- **Hidden Mode (HM).** Malicious nodes tunnel routing packets to each other without modification. As a result the wormhole nodes never appear in routing tables. If the wormhole example in Figure 1.1 is launched in HM, the fictive route will be A→#1→#7→D.
- **Participation Mode (PM).** The wormhole nodes process routing packets just like a normal MANET node, so the malicious nodes appear in an infected route as any pair of legitimate nodes, so the fictive route path for a PM wormhole will be A→#1→M_1→M_2→#7→D.

Both HM and PM wormhole nodes can also tunnel routing packets to each other by using one of the following two communication link types:

- **In-Band (I-B).** A malicious node forwards routing packets to the other wormhole node by tunnelling them through genuine network nodes, so in Figure 1.1, routing packets between M_1 and M_2 will be tunnelled through legitimate nodes #3, #4, and #5. This type of wormhole is easy to launch since a dedicated communication link between the wormhole endpoints is not required.
- **Out-of-Band (O-B**). This type of wormhole is more complex to launch since an external communication channel between the malicious nodes is needed, such as

network cable or directional antenna, but it attracts more traffic than an I-B wormhole since the link is significantly faster.

Originally, MANET routing protocols were designed on the assumption that malicious nodes did not exist in such environments and therefore included no security mechanisms. During the last decade, several secure routing protocols for MANETs have been proposed, either as stand-alone protocols (Sanzgiri et al., 2002) or more typically as extensions to existing routing protocols (Papadimitratos & Haas, 2003; Buchegger & Le Boudec, 2002; Hu, 2002; Hu et al., 2002; Papadimitratos & Haas, 2002; Zapata, 2002; Yi, et al., 2001) suggesting authentication, hashing techniques, encryption or digital signatures as preventive security mechanisms. Security attacks like wormholes cannot however, be realistically detected simply by using cryptography. In an open large-scale MANET, where nodes are allowed to join or leave at any time, trust in a node based on cryptography is difficult to realise in practice. Also, it must be taken into account that MANET nodes may consist of hardware restricted devices like sensors, small chips and actuators, on which the use of cryptographic measures would incur a significant computational cost.

An alternative approach for detecting malicious and selfish nodes in a MANET is to analyse either node behaviour or certain features of a route to build a reputation amongst nodes. These types of reputation/behaviour based security mechanisms can be classified as point detection algorithms, focusing on a single attack type, or more unified mechanisms, e.g. *intrusion detection systems* (IDS), being able to detect a range of attacks (Nadeem & Howarth, 2013). Several unified reputation-based security systems have been proposed for MANETs (Eissa et al., 2013; Saha et al., 2012; Buchegger & Le Boudec, 2002; Michiardi & Molva, 2002), though current systems do not cover all types of routing threats. Furthermore, many proposals require special types of nodes like guards or centralized nodes to be present in the network, which is impractical in a large-scale dynamic MANET.

Many security schemes have been proposed specifically for detecting wormhole attacks, although most solutions have some recurring limitations, such as the inability to detect all the wormhole variants defined above. Others require either dedicated hardware or make unrealistic assumptions about the network environment or the capability of the nodes and end up by imposing either high bandwidth loads on the network or computational overheads. A wide-ranging review of the state-of-the-art wormhole attack detection methods will be presented in Chapter 3.

1.2. Research Motivation

The lack of a single inclusive wormhole attack detection solution provided the motivation to investigate new potential detection mechanisms which are lightweight in terms of their computational complexity as well as network bandwidth load and have the ability to detect all wormhole variants. In the literature, several types of route or node features have been utilized for identifying wormholes or wormhole nodes, such as *received signal strength indicator* (RSSI) (Jain et al., 2012), *number of neighbours* (Song et al., 2012), *network visualization* (Lu et al., 2013), *frequency of node appearances in routes* (Su, 2010), *HC* (Jen et al., 2009), *geographical location information* (García-Otero & Población-Hernández, 2012), and *packet delay* (Khabbazian et al., 2009; Chiu & Lui, 2006). Most of these features however, are unsuitable for analyzing the existence of all wormhole variants and some are based on unrealistic assumptions as will be highlighted in Chapter 3. The focus of many proposed wormhole detection schemes is on packet delay analysis and involves measuring the delay incurred by sending a packet to either neighbouring nodes or alternatively over multiple hops. If the delay is unrealistically high it may be inferred that a wormhole exists between two disjoint neighbors or on a route. These types of detection schemes are attractive since they are efficient, easy to implement, and are thus applicable on a wide range of network devices. However, current solutions rely either on some impractical or unrealistic assumptions, typically that packet processing delays at each node are approximately the

same, since *round trip time* (RTT) measurements are used or they are only applicable to specific wormhole types under certain network conditions. In a real-world MANET, differences in node hardware and potential queuing delays at nodes will inevitably lead to variations in packet processing delays and so RTT alone is not sufficiently accurate to identify for example, a PM O-B wormhole, which has a fast link.

The lack of unified and robust wormhole detection technique allied with the appeal and potential that packet delay based schemes afford, provided the context for the overarching thesis research question and related objectives, which are now formally defined.

1.3. Research Questions and Objectives

From the discussion in Section 1.2, the following main research question addressed in this thesis was framed:

> ***How can wormhole attacks be accurately detected in a generic MANET with minimal network overheads?***

Following a detailed literature review to survey existing wormhole detection solutions, packet delay analysis was identified as a fertile area for further investigation in seeking to develop a unified detection framework which can offer accurate performance across a variety of network scenarios. The following key specifications for this new framework were formulated:

- Detects all existing wormhole types
- Easy to implement with NO additional hardware requirements.
- Low cost in terms of computational complexity, network bandwidth load, and *false positive* (FP) detection.

- Independent of network topology and adaptive to various network environments, like indoors and outdoors, which lead to variability in node radio ranges.
- Resistant to malicious packet delay time measurement tampering.

Three objectives were framed based on these requirements as well as underpinning the overarching research question, and three original contributions presented in this thesis to fulfill these objectives as outlined in Figure 1.2.

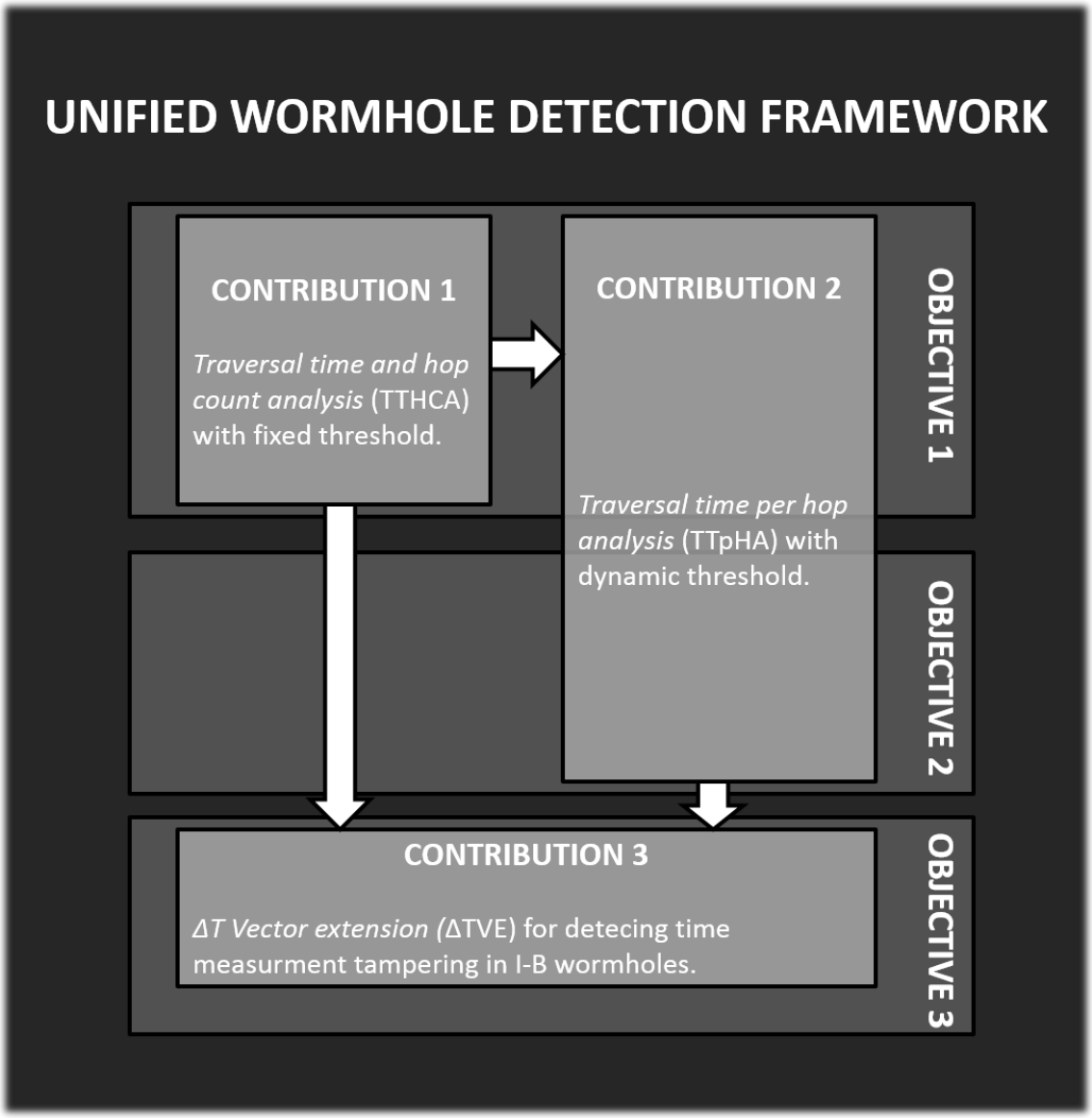

Figure 1.2: Layout of the objectives of the wormhole detection framework and contributions for fulfilling these.

The objectives and their justifications will now be presented, while the resulting framework contributions are surveyed in the next Section:

1. *To investigate the development of a novel robust wormhole attack detection model based upon packet delay analysis.*

Justification: Building on the compelling reasons detailed in Section 1.2, this objective critically evaluates the potential of developing a new lightweight robust wormhole attack detection model using packet delay analysis. A new algorithm called *traversal time and hop count analysis* (TTHCA) (Karlsson et al., 2011) is designed within a MANET simulation environment, initially under the assumptions of identical node hardware and a *line-of-sight* (LOS) scenario within a homogeneous network arrangement where LOS refers to nodes being located in an open space environment, i.e., outdoors or in a large room, where the nodes have direct visible contact with each other.

2. *To design an adaptive mechanism for the framework to manage dissimilar node hardware and variable radio coverage.*

Justification: High fluctuations in radio ranges can be anticipated in heterogeneous MANETs comprising nodes with dissimilar wireless hardware and antennae located in obstructed environments. This makes wormhole attack detection based on packet delay analysis more challenging than in a homogeneous, direct LOS network environment. This objective critically analyses the impact of relaxing the two assumptions made in *Objective 1* on node hardware and network environment, by developing a new wormhole identification process which employs a dynamic threshold to enable the algorithm to automatically adapt to prevailing network conditions.

3. *To critically analyse the conditions for malicious tampering of packet delay measurements and to frame suitable mitigation strategies.*

Justification: Packet delay measurements can potentially be altered by malicious nodes to prevent wormhole attack detection. This objective firstly analyses the specific conditions that must exist and the corresponding impact of packet delay time measurement tampering on the wormhole attack detection performance of the new framework. Innovative strategies will then be advanced to successfully prevent time tampering attacks while concurrently retaining low false positive detection performance.

1.4. Contributions

This thesis presents a new unified wormhole attack detection framework which is effective for all wormhole types, is lightweight, and generates low FP rates. The framework, shown in Figure 1.2, makes a number of innovative contributions to the field. To fulfil *Objectives 1* and *2*, two contributions in MANET wormhole attack detection based upon packet delay analysis are proven. The first is the TTHCA (Karlsson et al., 2011) algorithm, which measures and analyses the overall route *packet traversal time* (PTT) which better reflects the route distance since RTT may have high variance due to variable packet processing delays at intermediate nodes. If PTT in relation to the route HC is greater than a predefined static threshold, then a wormhole is suspected to exist on the found route. In homogeneous LOS environments, where the variation in node radio range coverage can reasonably be assumed to be low, TTHCA satisfactorily fulfils *Objective 1* as will be shown in Chapter 5.

In the second contribution, the initial LOS and identical node hardware assumptions are relaxed and the corresponding performance of using the fixed detection threshold in TTHCA is critically evaluated. To fulfil *Objective 2*, a modification to TTHCA is introduced called *traversal time per hop analysis* (TTpHA) (Karlsson et al., 2016), which uses a dynamic

threshold for the maximum permissible PTT per hop. This renders TTpHA significantly more flexible than TTHCA, since it can now automatically adapt to prevailing network conditions as well as tolerate higher radio range variations.

The third novel contribution critically analyses the prevailing conditions for successful tampering of PTT measurements by a malicious node, with the explicit aim of preventing either TTHCA or TTpHA from detecting a wormhole. An extension, called Δ*T vector (*ΔTVE*)* (Karlsson et al., 2013), is then proposed, which can be seamlessly integrated into both TTHCA and TTpHA to automatically detect time tampering attacks in PM I-B wormholes by applying statistical analysis of collected packet processing delay measurements. This contribution partially fulfils *Objective 3* since it does not consider PM O-B wormholes.

1.5. Thesis Structure

The rest of the thesis is organized as follows:

- **Chapter 2** presents a rigorous and generic literature review on MANET routing security research. A survey on MANET routing protocols as well as established routing attacks is given and a critical review on security extension proposals is provided. Work from this Chapter has been published in Karlsson et al. (2012).
- **Chapter 3** focuses specifically on the state-of-the-art of wormhole attack detection research. Existing detection schemes are classified into categories according to their approach and their comparative advantages and disadvantages, and gaps in the field identified.
- **Chapter 4** explains the research methodology adopted in this thesis, the choice of simulation test platform, the performance metrics and the software code validation as well as statistical significance verification processes pursued to ensure the correctness of the new framework.

- **Chapter 5** introduces the TTHCA wormhole detection algorithm and critically evaluates its wormhole detection performance in comparison to RTT and HC analysis based schemes. Work from this Chapter has been published Karlsson et al. (2011).
- **Chapter 6** critically analyses the limitations of the fixed threshold for determining the maximum permissible PTT/HC used in TTHCA and introduces a new, more flexible TTpHA wormhole detection algorithm that is able to automatically adapt its performance to prevailing network conditions. Work from this Chapter has been published in Karlsson et al. (2016).
- **Chapter 7** evaluates the feasibility for a wormhole node to tamper with the PTT measurements in TTHCA and TTpHA in order to prevent wormhole detection. A security extension called ΔTVE is proposed for the detection of such time tampering attacks. Work from this Chapter has been published in Karlsson et al. (2013).
- **Chapter 8** discusses future research avenues for exploiting key features of the new framework, including their possible integration with existing machine learning based IDS to create a single system for detecting the most severe routing security threats.
- Finally, **Chapter 9** concludes the key findings and original contributions presented in this thesis.

In the next Chapter, a critique of the literature relating to firstly general MANET routing security research is presented, before specifically focusing upon wormhole attacks and existing techniques for their effective detection.

2. MANET ROUTING SECURITY: A LITERATURE REVIEW

2.1. Introduction

MANETs have no fixed infrastructure and are therefore more vulnerable to routing attacks than infrastructure networks. Since dedicated routers are missing in MANETs, each node takes part of the routing process and in a dynamic network, where nodes are continuously joining and leaving the network, it is difficult to discern nodes with malicious intention from normal routers. In this Chapter an overview of the most known attacks/threats on MANET routing as well as proposed security protocols/extensions is presented. To provide a better understanding of the routing attacks, an overview of existing MANET routing protocols is first given.

2.2. Overview of Routing Protocols

Several routing protocols have been proposed for MANETs in recent years. These can broadly be classified in table driven/proactive, on-demand/reactive, and hybrid routing protocols. Examples of well-known protocols from each category will now be individually examined.

2.2.1. Table driven/Proactive Protocols

These use a proactive routing scheme, so every node in the network maintains consistent up-to-date routing information from each node to all other nodes in the network. Table driven routing protocols have a low route acquisition delay because every node always has a fresh route available to all other nodes in the network. However, the requirements on storage, bandwidth, and power are high since each node must always keep its routing table up-to date (with route information to all other nodes) which requires periodical exchange of routing messages. Examples of well-known table driven protocols are the highly dynamic

destination-sequenced distance vector routing (DSDV) (Perkins & Bhagwat, 1994) and *optimized link state routing* (OLSR) (Clausen et al., 2003).

Destination-sequenced Distance Vector routing (DSDV)

DSDV is one of the originally proposed MANET routing protocols. It is based on the distributed Bellman-Ford distance vector algorithm where the main contribution is to solve the routing loop problem by using a sequence number for each routing entry. Routing tables are generated and maintained by periodically exchanging routing messages among neighbours. Apart from the destination each entry in a routing table consists of the next hop to reach it, the route HC, the sequence number generated by the destination, the install time (which is the time when the entry is made), and stable data. Install time is used for identifying obsolete routes, i.e. a route which has not been updated for a certain period of time and which will be removed from the routing table. The stable data entry is a metric for determining the stability of a route.

A major advantage of DSDV is that each node always knows the next hop on the path to all destinations in the network which means that minimum time is consumed for setting up a route. A disadvantage on the other hand is that regular updates of routing tables consume battery power and network resources even when the MANET is idle. Furthermore, DSDV is not suitable for dynamic and large scale networks as a new sequence number is necessary before the network re-converges whenever the topology of the network changes.

Optimized Link State Routing (OLSR)

OLSR is a modification of basic link state routing optimized for MANETs. In link state routing, each node exchanges messages with all nearby nodes for discovering its neighbours. This information is then distributed to all other nodes by flooding control messages into the network. To reduce control traffic overhead in OLSR, a node only distributes control

messages to a preselected set of neighbours called *multipoint relays*. This saves network resources since it prevents the same control message from being distributed multiple times to the same region. When each node has received the topology information of the MANET it can calculate the shortest HC route to all other nodes.

2.2.2. On-demand/Reactive Protocols

On-demand protocols are based on a reactive routing scheme, so a route is established only when needed. On-demand protocols place a much lower load on the network, compared to table driven, since each node need not constantly keep own routing tables up-to-date. However, route acquisition delay is high since routing messages must be exchanged every time before communication is possible over a new route. On-demand routing protocols are though more suitable than table-driven for dynamic network topologies. Two prominent MANET routing protocols, based on reactive routing schemes are *dynamic source routing* (DSR) (Johnson & Maltz, 1996) and *Ad hoc On-demand Distance Vector* (AODV) (Perkins & Royer, 1999) which will now be respectively considered.

Dynamic Source Routing (DSR)

To set up a link to the destination node, the source node floods the network with a *route request* (RREQ) message. If a node receiving this RREQ is neither the destination nor has a fresh route to the destination, then it adds its own address to the RREQ packet before broadcasting it to neighbouring nodes. Each intermediate node also caches all node addresses received in the RREQ packet, i.e. the path to the source node. If the receiver of a RREQ is the destination node it adds its own address information to a new *route reply* (RREP) packet which is sent back to the source node as a unicast packet through the nodes listed in the RREQ. As during the RREQ broadcast, each node receiving a RREP caches the node addresses received in the RREP before adding its own address to the packet. As a result, when the RREP reaches the source node, all intermediate nodes have registered a fresh route

to both source and destination nodes. The destination node replies to each RREQ it receives and hence, the source node will know more than one route to the destination node upon reception of all RREP packets. The advantage of registering multiple routes to a destination node in the routing table is that if a link fails, the source node does not need to re-initiate the route discovery process. Instead it chooses an alternative route from its routing table. However, in highly dynamic MANET topologies, cached routing information may become obsolete in a short period of time.

Ad hoc On-demand Distance Vector (AODV)

To set up a new route in AODV, the source node initiates the route discovery process by flooding the network with a RREQ message such as in DSR. In contrast to DSR, node address information is not added to the RREQ packet. Instead, each intermediate node and the destination node creates a reverse route to the source node when receiving a RREQ, i.e. registers the previous hop, from which it received the RREQ, as next hop towards the source node. If the receiver of a RREQ is the destination node it sends a RREP message back to the source as a unicast packet over the shortest route and each intermediate node receiving the RREP registers the next hop information to the destination node in its routing table. As a result, when the RREP reaches the source node, all nodes in the shortest route path will have a route both to the source and destination. In contrast to DSR, a destination node only replies to the first RREQ message it receives and therefore there will be only one registered route between the source and destination nodes. While DSR incurs a lower routing overhead due to its multiple route feature, AODV still provides superior performance in highly dynamic MANET environments. It is also the most popular on-demand routing protocol (Zhong et al., 2015) with most existing routing protocol versions and security extensions being based around it, including the framework developed in this thesis.

2.2.3. Hybrid Protocols

A hybrid routing protocol is a combination of proactive and reactive schemes with the aim of exploiting the advantages of both types. A proactive scheme is used to discover routes to nearby nodes and reactive schemes are used to discover long distance nodes. An example of a hybrid routing protocol is *zone routing protocol* (ZRP) (Haas et al., 2002). ZRP can also be categorized as a hierarchical routing protocol where the network can be grouped in to clusters, trees, or zones, where one node is chosen to be a leader that manages that particular routing area.

Hybrid protocols incur less route acquisition delay than reactive protocols and a lower overhead than proactive protocols. They are however, not suitable for highly dynamic MANET environments since in such network conditions, it is not feasible to delegate roles to nodes and segment the network into zones.

2.3. Overview of Routing Security Attacks

Due to the self-configuring nature of a MANET, each node participates in the routing process in addition to its other activities and there are no dedicated routers in the network. This causes a significant security threat especially in highly dynamic MANETs where a large number of network nodes can join and leave the network so it is impossible to know in advance whether a node is a trustable router or not.

Security attacks in MANET routing can be divided in two main types; passive and active. The intention of a passive attack is typically to listen and retrieve vital information inside data packets, for example by launching a traffic monitoring attack. In such an attack, a malicious node tries to identify communication parties and functionality which can provide

information to launch further attacks. The attack is called passive because the normal functionality of the network is not altered.

An active attack is performed by a malicious node with the intention to interrupt the routing functionality of a MANET. Examples of active attacks are (Karlsson et al., 2012; Soni et al., 2010):

- Modification attacks
- Impersonation attacks
- Fabrication attacks
- Rushing attacks
- Wormhole attacks
- Replay Attacks
- Selfish behaviour

2.3.1. Modification Attacks

This is typically launched by a malicious node with the deliberate intention of redirecting routing packets, by for example modifying the HC value of a packet to a smaller value. By decreasing the HC value, a malicious node can attract more network communication. A typical modification attack is the *black hole attack* (Hongmei et al., 2002) where a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. As a result, the target node will send its packets through the malicious node when communicating with the destination node. The malicious node can choose to either drop the packets or place itself on the route as the first step in what is known popularly as the *man-in-the-middle* (MITM) attack**.** A modification attack can also be a special kind of *denial-of-service* (DoS) attack. In this situation the intention is to destruct the entire routing function by for instance altering the source routes in the header of the routing

packet. This type of DoS attack however, is only effective on routing protocols where intermediate nodes are included in the packet header, such as DSR.

2.3.2. Impersonation

In this type of attack (also known as spoofing), a malicious node uses for example the IP address of another node in the outgoing routing packets. As a result, the malicious node can receive packets meant for the other node or even in the worst case, completely isolate that node from the network.

2.3.3. Fabrication

The main purpose of fabrication attacks is to drain off limited resources in other MANET nodes, such as battery power and network connectivity by for example flooding a specific node with unnecessary routing messages. A malicious node can for example, send false *route error* (RERR) messages. This kind of attack is more prominent in reactive routing protocols where path maintenance is used to recover broken links.

In a fabrication attack a malicious node can also attempt to create routes to nodes that do not exist. As a result, the routing table of a neighbour node can become full which prevents it from registering any new routes. This type of fabrication attack is however, only effective on table-driven routing protocols where each node in the network keeps an up-to-date route to all other nodes in the network.

A fabrication attack can also be launched by a selfish node that duplicates the transmission of packets to another node, just to ensure all packets reach the destination node. This behaviour may lead to an excessively high network traffic load.

2.3.4. Rushing Attacks

This is a DoS attack effective on reactive routing protocols. Under normal circumstances the *medium access control* (MAC) layer impose delays between the instant the packet is delivered to the network interface for transmission and the moment when the packet is actually transmitted. Reactive routing protocols normally specify a delay between receiving and sending a RREQ packet for avoiding collisions. In a rushing attack a malicious node ignores these delays with the intention to achieve fast forwarding of RREQ messages. By doing so it will attract more routes than nearby nodes since most reactive routing protocols only process the first received RREQ messages meaning that the messages received later from legitimate nodes will be ignored. A malicious node can also obtain faster RREQ forwarding than its neighbours by flooding them with data packets to keep their queues full. A more powerful rushing attack can also be achieved by employing a wormhole attack, which will be described next.

2.3.5. Wormhole Attacks

A wormhole (Hu et al., 2003) is a particularly severe attack on MANET routing. A malicious node captures packets from one location in a network and tunnels them to another malicious node, located several hops away, which forwards the packets to its neighbouring nodes. This creates the illusion that two endpoints of a wormhole tunnel are neighbours even though they are located far away from each other in reality. A strategic placement of a wormhole causes most of the network traffic to go through the malicious nodes. Once the wormhole link is successfully established, further attacks can be launched by the malicious nodes such as selective packet drop to disrupt communication or data sniffing in order to capture confidential information.

There are two classes of wormhole attacks (Khabbazian et al., 2006): HM and PM. In the former, HM wormhole nodes are invisible from legitimate nodes as they do not process

routing packets. They simply capture, tunnel and forward packets to each other and never appear in routing tables. In contrast, PM wormhole nodes are visible during the routing process since they process routing packets as any normal node. Aside from relaying routing packets to its neighbours, a PM wormhole node tunnels routing packets to the other PM node, giving it the opportunity to deleteriously control network performance**.**

A shortcut link between two HM or PM wormhole nodes can be established using either an I-B or O-B channel (Mahajan et al., 2008). An I-B channel is one where the wormhole nodes tunnel packets to each other through legitimate nodes in the network, while an O-B channel connects the two malicious nodes through an external communication link like a network cable or directional antenna.

2.3.6. Replay Attacks

In this kind of attack, a malicious node records routing information messages sent from neighbour nodes and resends them later to other nodes. Since MANETs typically do not have a fixed topology, nodes receiving maliciously replayed routing messages will store old information in their routing tables. As a consequence, major disturbance of the MANET routing operation may be caused.

2.3.7. Selfish Behaviour

Selfish behaviour means a node does not wish to cooperate in any routing. It may for example be that it wants to save energy and so switches to a “sleep mode” whenever it is not taking part in any network communication. While such an attack may not be launched with explicitly malicious intentions, it can lead to serious disruptions in network communications such as high route discovery delays and dropped data packets. If the selfish node also happens to be the only communication link between two MANET endpoints, communications between these endpoints will be become unavailable.

2.4. Survey of Secure Routing Protocols

Most routing protocols have originally been designed without taking security into account. It was assumed that all nodes in a MANET were trusted. However, this is not the case in a large scale and dynamic MANET and if the routing protocol is unprotected, the whole MANET can be liable to several different types of security attacks. A lot of research has been done in the area of MANET routing security and several secure versions have been derived from current routing protocols to provide secure MANET routing protocols (Koul & Sharma, 2015; Karlsson et al., 2012). The purpose of this Section is to present an overview of well-known secure routing protocols that have been developed with the intention to provide protection against a range of security attacks. These can mainly be divided in cryptographic based, reputation based or a combination of both.

2.4.1. Secure Routing Protocols based on Cryptography

Cryptography can be used for preventing external attacks, such as modification, fabrication, impersonation and rushing. Several existing secure routing protocols propose node authentication, hashing techniques, encryption and digital signatures for protecting against routing attacks. Some of these protocols will now be critically evaluated.

Secure AODV (SAODV) (Zapata, 2002)

This protocol was introduced to protect the routing messages of the AODV protocol. In SAODV, hash chains are used to authenticate the HC fields within the RREQ and RREP packets. Since all other fields of the RREQ message are non-mutable they can be authenticated by verifying the signature in the RREQ. The RREQ message is signed by the private key of the source node and the RREP message is signed by the private key of the destination node. By doing so, both the source and the destination nodes can identify their communication partners and thus avoid impersonation attacks. SAODV also prevents most modification attacks since both the non-mutable and the HC field in the routing packets are

protected. The intermediate nodes verify their signatures in both the RREQ and RREP messages as well, and only store a forward or reverse route entry in the routing tables, if the signature in the routing message is verified so routes to unauthorized nodes are not permitted.

By using digital signatures in the RERR packets SAODV can also prevent malicious nodes from forging RERR message, which is a type of fabrication attack. Replay attacks are also prevented by SAODV since in AODV only routing packets with unique sequence numbers are processed and the sequence number field in the routing packets cannot be altered by a malicious node. However, since only the end nodes (source and destination) are authenticated, attacks not requiring false modifications of the routing packets, such as rushing attacks, wormhole attacks, and selfish behaviour cannot be detected by SAODV.

Ariadne (Hu, 2002)

This is a secure reactive routing protocol based on DSR that provides authentication of routing messages. Authentication can be performed by using shared secret keys between each pair of nodes, shared secret keys between communicating nodes combined with either broadcast authentication or digital signatures. Ariadne is based on the *timed efficient stream loss-tolerant authentication* (TESLA) protocol (Perrig et al., 2005) which is a broadcast authentication procedure requiring relaxed time synchronization. It consists of two steps; *routing message authentication* and *routing header verification*

During the *routing message authentication* step, a node forwarding a RREQ message indicates a *message authentication code* (which throughout the thesis is abbreviated as **MAC** not to confuse it with *medium access control* (MAC)) which is computed with a shared secret key over a time stamp (or other unique data). The receiver of the message can then authenticate the message by using its own shared secret key. *Routing header verification*

includes per-hop hashing to verify that no hop has been omitted, i.e. no node has been removed from the source root (list of intermediate nodes) included in the routing packet.

Due to the authentication of routing messages, and prevention from false modification of the source route and HC field, Ariadne provides protection from all routing attacks described in the previous Section, except selfish behaviour, under the assumption that none of the nodes owning legitimate shared keys, are malicious. In addition to PM wormholes, Ariadne can also provide protection from HM wormholes, when used with the *TESLA instant key disclosure* (TIK) protocol for precise time synchronization between neighbour nodes.

Authenticated Routing for Ad hoc Networks (ARAN) (Sanzgiri et al., 2002)

The purpose of this protocol is to detect and protect against malicious actions by third parties and peers. It provides authentication, message integrity and non-repudiation. ARAN can be used in two different security stages; a simple mode which is mandatory and an optional stage which provides stronger security but also more overheads. It is not suitable for mobile devices with very low processing or battery capacity. ARAN uses digital certificates for authentication and non-repudiation. Each routing message is signed by the source node and broadcasted to all neighbours. An intermediate node removes the certificate and signature of the previous hop and replaces them with its own.

Due to the strong authentication, message integrity and non–repudiation ARAN affords like Ariadne, effective protection from all the attacks described in Section 2.3. However, due to heavy asymmetric cryptographic operations and large routing packets, ARAN has a high computational cost for route discovery. Another drawback of ARAN is vulnerability to selfish nodes and HM wormhole attacks.

Security Aware Ad hoc Routing (SAR) (Yi et al., 2001)

This protocol incorporates security attributes as parameters in MANET route discovery. It enables the use of security as a negotiable metric with the intention to improve the relevance of the discovered routes. While AODV discovers the shortest path between two nodes, SAR can discover a path with desired security attributes. For instance, the criterion for a valid route can be that every node in the route must own a particular shared key. In such a case, routing messages would be encrypted with the source node's shared key and only the nodes with the correct key can read the header and forward that routing message. As a result, if a routing message reaches the destination, it must have travelled through nodes having the same trust level as the source node. It is then for the node initiating the route discovery to decide upon the desired security level for that route.

SAR has been presented as an extension to AODV but it can also be extended to any existing routing protocol. Due to the strong cryptographic protection of routing messages modification, impersonation, rushing, fabrication, replay and PM wormhole attacks are effectively eliminated. A major problem with SAR however, is that it involves a significant encryption overhead since each intermediate node has to perform both encryption and decryption operations. As with all other cryptography-based secure routing protocols, HM wormhole nodes and selfish nodes cannot be detected using this protocol.

Secure Efficient Ad hoc Distance Vector (SEAD) (Hu et al., 2002)

SEAD is a proactive routing protocol, based on DSDV, that uses a hash chain method for verifying the authenticity of the sequence number and route metric elements of the routing packets. SEAD thus provides protection against attackers trying to create incorrect routing state in other nodes. SEAD requires authentication of the source to ensure that routing information has been received from a legitimate node which prevents impersonation attacks. One way of performing source node authentication in SEAD is to set up a shared secret key

between each pair of nodes in the MANET. This key is then used for **MAC** calculations between the nodes for authenticating a routing update message.

A limitation of SEAD is that the next hop or destination field of a routing update packet is not protected and thus modification attacks are only partially eliminated. Furthermore, even though the sequence number is authenticated, SEAD does not recognize packets sent multiple times with the same sequence number and is thus vulnerable to replay attacks.

Secure Routing Protocol (SRP) (Sanzgiri et al., 2002)

This is a protocol designed for ZRP but it can also be used with pure reactive routing protocols. In ZRP, a *security association* (SA) is required between each source and destination node. It is assumed that the SA can be established by using a shared key between the two communicating nodes. The shared key is negotiated based on the other party's public key. SRP uses an additional header to the underlying on-demand routing protocol packet. The header contains a sequence number, an ID number and a **MAC** field where the output of a key hashed functions is inserted. RREQ messages are discarded by intermediate nodes if the SRP header is missing.

When the RREQ message has reached the destination node it verifies if it has a SA with the source node. The RREQ packet is dropped if the sequence number is greater or equal to a maximum value since it is then considered to be replayed. If the sequence number is valid, the destination calculates the keyed hash of the request fields and compares the output with the **MAC** field of the SRP header. If they match the authenticity of the sender and the integrity of the request message are verified and the destination generates a RREP message where it includes the path information from the source to destination node, the ID and sequence number.

The source node validates the sequence number and the **MAC** field in the same way as the destination node. The source node also compares the source route (path information) included in the reply message with the reverse of the route carried in the reply packet. If they match, it can be assumed that the route information in the routing packet has not been altered.

In SRP, intermediate nodes are not authenticated so SRP is vulnerable to routing attacks not requiring false modification of routing packets, including all wormhole types and selfish behaviour.

2.4.2. Reputation based Secure Routing Protocols

Some routing attacks like selfish behaviour, cannot be detected using cryptography and in an open large scale MANET, where any node is allowed to join or leave at any time, trust in a node based on cryptography is difficult to realise in practice. Another approach for detecting malicious and selfish nodes in a MANET is to analyse the behaviour of the nodes and based on that create lists where the trust against other nodes are weighted. In this subsection, a few examples of reputation based secure MANET routing protocols are examined.

Cooperation of Nodes: Fairness in Dynamic Ad hoc NeTworks (CONFIDANT)

(Buchegger & Le Boudec, 2002)

The main idea of CONFIDANT is to make non-cooperative nodes unattractive for other nodes to communicate with. A node chooses a route based on trust relationships built up from experienced, observed or reported routing and forwarding behaviour of other nodes. Each node observes the behaviour of all nodes located within the radio range. When a node discovers a misbehaving node, it informs all other nodes in the network by flooding an alarm message. As a result, all nodes in the network can avoid the detected misbehaving node when choosing a route.

CONFIDANT consists of the *monitor*, *reputation system*, *path manager* and *trust manager* components. The *monitor* component listens to its neighbours and inspects if they forward a routing packet that has been sent to them and thus detects non-cooperative nodes such as selfish nodes. The monitor can also check whether a forwarded packet is modified according to the routing protocol, if not then a modification attack is suspected. The *trust manager* is responsible for sending and receiving alarm messages which are sent by nodes suspecting malicious behaviour in a certain node. The *reputation system* maintains a table with node ratings and the path manager component manages route information according to feedback from the reputation system.

A major weakness of CONFIDANT is that an attacker is able to send false alarm messages, and as a consequence the attacker can claim that a node is misbehaving even if that is not true. No wormhole is detected due to the fact that they do not either drop or falsely modify routing packets during the route discovery procedure. Furthermore, CONFIDANT has no capability for detecting impersonation, replay, rushing or fabrication attacks.

Collaborative Reputation Mechanism to Enforce Node Cooperation in MANETs (CORE) (Michiardi & Molva, 2002)

CORE is similar to CONFIDANT but employs a more complicated reputation exchange mechanism. Reputation is divided into three distinct components; *subjective reputation*, *indirect* and *functional*. *Subjective reputation* is created through their own observations, *indirect reputation* is built based on reports from other nodes, and *functional reputation* is based on behaviour monitored during a specific task. All these reputations together are weighted for a combined reputation value. The major difference between CORE and CONFIDANT is that CORE only allows positive reports while CONFIDANT also accepts negative reports. As a result, in CORE it is not possible to decrease the popularity of a certain node by sending false reports.

Friendship-based AODV (FrAODV) (Eissa et al., 2013)

FrAODV is a trust based security extension for AODV where each node maintains a list of friends and a friendship value for each friend. The friendship value can range from 0 to 100 where 100 refers to the highest level of trust. Three features, i.e. *packet precision*, *blacklists* and *trust value metric* are used to assess the level of trust for each node (Samian et al., 2008). *Packet precision* means the accuracy of a routing packet forwarded by a neighbouring node, which can be used for example, to detect malicious modifications of routing packets, while a node will be listed in a blacklist if it does not forward a routing packet it has received and can thus be suspected as a selfish node. *Trust value metric* means the use of discrete values to define the trust level of a node.

Trusted routes are built by two algorithms, i.e. *RvEvaluate* and *FwEvaluate*. The *RvEvaluate* algorithm builds up a trusted reverse route from the destination and intermediate nodes to the source node. When an intermediate node receives a RREQ its previous and next hop node's friendship value is evaluated and the RREQ is rejected if either of these values are less than a *threshold for friendship* (TF) value. If the friendship value is greater than TF the friendship value of the whole reverse route, i.e. the average friendship value of all nodes on the reverse path between the current and source nodes, is calculated. If the friendship value of the reverse route is greater than a possible previous reverse route to the source, the intermediate node updates the previous route with the new route in its routing table. When a destination node receives a RREQ the procedure is the same, except that the friendship value is only evaluated for the previous hop. Similarly, the *FwEvaluate* algorithm builds up a trusted forward route from the source and from an intermediate node to the destination node upon receiving a RREP.

FrAODV has no measures for detecting routing attacks that do not modify or drop routing packets such as malicious nodes distributing false RERR messages (fabrication), rushing,

replay and wormhole attacks. Node authentication mechanisms are also missing, which means that spoofing is possible.

2.4.3. Secure Routing Protocols based on a Combination of Cryptography and Reputation

Several secure MANET routing protocols propose a combination of cryptography and behaviour analysis for providing broader protection features. A critical review of these will now be presented.

Two-level Secure Re-routing (TSR) (Saha et al., 2012)

This scheme, which is designed for the DSR protocol, detects attacks at the transport layer and responds to them at the network layer. TSR implements four modules, i.e. *local supervision* (LS), *node isolation algorithm* (NIA), *congestion windows surveillance* (CWS) and *alternate route finder* (ARF).

Initially a data structure of one-hop neighbours is built at each node by broadcasting HELLO messages to which the neighbours respond. The neighbour nodes then exchange theirs lists of one-hop neighbours to which each node can supplement its data structure with also its two-hop neighbour information. After this process a packet will not be forwarded to a node that is not in the neighbour list and correspondingly a packet received from a fake neighbour will be dropped. Also if a routing packet is received where the previous hop field is not in the list of two-hop neighbours, the packet will be discarded.

After successful neighbour discovery, the LS module can monitor incoming and outgoing traffic of neighbours. In TSR, a node that is a neighbour of two successive nodes A and B obtains the role of a watch node for A and B. The watch node records all information sent from A to B and stores it in a watch buffer. The stored information includes for example; packet source, type, identification, next hop and previous hop. The watch node examines

each packet that the monitored node forwards and compares it with the watch buffer. A malicious counter for each monitored node at the watch node is incremented for each detected malicious behaviour.

When the malicious node counter for example, of monitored node B exceeds a threshold, the NIA module at the watch node revokes B from its list of neighbours and sends an alert message to all neighbours of B. This alert message is authenticated using a shared key between the watch node and all receivers of the alert.

After receiving alert messages about a node B the receiver invokes the CWS module to verify if B really is malicious. This is a process performed at the transport layer where variations in the size of the TCP congestion window are used to detect abnormalities. If a node on a path is verified to be malicious the ARF module is invoked to find an alternative route between the source and the destination avoiding the malicious node.

Secure Link State Routing Protocol (SLSP) (Papadimitratos & Haas, 2003)

The main functionality of SLSP is to secure the discovery and distribution of link state information by using asymmetric keys. SLSP consists of three major steps: *public key distribution*, *neighbour discovery* and *link state updates*. Public keys are distributed between a node and all its neighbours. A central server for key distribution is thus not needed. Periodic hello messages, used in neighbour discovery, are signed using the private key of the sender. Signed link state update messages are identified by the IP address of the initiating node and include a sequence number. A node receiving a link update messages verifies the attached signature using the public key it received earlier during the public key distribution phase. The HC in the update message is protected by using a one-way hash chain.

DoS attacks are avoided in SLSP since each node maintains a priority ranking of their neighbour nodes based on the rate of control traffic they have observed. Neighbour nodes that generate update packets with the lowest rate are given highest priorities. Thus, malicious neighbours generating a huge amount of unnecessary update packets will get the lowest priority which limits the effectiveness of a DoS attack.

Secure Routing Against Collusion (SRAC) (Yu et al., 2009)

This is a secure routing protocol in which each node makes a routing decision based on the trust and performance of neighbour nodes. This trust is built by performing continuous observations on incoming and outgoing packets to/from neighbouring nodes. Pair-wise secret keys between the source, intermediate nodes and the destination are then used to protect route discovery messages. The route discovery process is performed as follows; the source node chooses a random number which it signs with its private key and then a key hash function is used to protect the route discovery message. The signature and the key hash value is appended to the route discovery message being sent hop by hop to the destination. In a route, the nodes with the highest level of trust are chosen first. If the trust level is the same for two or more nodes then the choice of path is based on HC information. If the HC is also the same, then the route is chosen based on the nodes' performance.

Due to strong cryptographic protection of routing packets in combination with monitoring of neighbour node behaviour, SRAC provides protection against modification, impersonation, rushing and replay attacks as well as selfish behaviour. However, RERR packages are not protected and thus SRAC is vulnerable to RERR packet related fabrication attacks.

Trusted AODV (TAODV) (Li et al., 2004)

The main purpose of TAODV is to provide a trust model for the AODV routing protocol

presented earlier in Section 2.2.2. It assumes each node is equipped with monitoring mechanisms or intrusion detection units so that it can check the behaviour of its neighbours. Trust among nodes is represented by an opinion derived from subjective logic (Jøsang, 2001). These opinions are dynamic and updated frequently. A node performing normal communications will have its opinion from another node's point of view increased and correspondingly decreased as a result of some malicious behaviour. TAODV also implements a trust recommendation mechanism to exchange trust information amongst nodes.

TAODV recommends that a cryptographic security protocol, such as Ariadne (Hu, 2002), is used in combination with TAODV so that nodes can be authenticated e.g. through digital certificates, when the MANET is initiated and before nodes have established trust relations among one another through TAODV. A prominent feature of TAODV is that there is no need to request and verify certificates once the trust relations are established, which significantly reduces the computational overheads.

Friend-based Ad hoc Routing using Challenges to Establish Security (FACES) (Dhurandher et al., 2011)

FACES is a MANET routing protocol where secure routing is established by means of four steps; *i) challenge the neighbour*, *ii) rate friends*, *iii) share friends* and *iv) route through friends*. Each node maintains an *unauthenticated list* containing nodes of which no security information is present, a *question mark list* with suspicious nodes and a *friend list* consisting of trusted nodes rated on a scale of 0 to 10.

The *challenge the neighbour* step is used to establish trust for a new node and consists of a basic test to complete for proving honesty and integrity. Before the new node is challenged, it is listed in the neighbour nodes' *unauthenticated list*. Then, one of the neighbouring nodes

challenges the new node by first performing the *share friends* stage to which the new node responds with either its *friends list* or *unauthenticated list,* if the *friend list* is empty. From the received *friends list*, the neighbouring node chooses a destination node to which it already has a safe route and exchanges challenge and response messages with that node through both the new node and a trusted intermediate node. Public key cryptography is applied for encrypting these messages. If the responses received from both the trusted intermediate node and the new node are the same then the neighbouring node adds the new node to the bottom of its *friend list*. As a result of this procedure the neighbouring node can ensure that the new node behaves genuinely, at least initially. If no response is received from the new node or if the response received from the new node does not match the one received from the trusted intermediate node then is considered suspicious and added to the *question mark list.*

Nodes on the friends list are rated on a scale of 0 to 10 and has three classes of ratings, i.e. *data rating* (DR) based on the amount of data a friend node has successfully transferred, *friend rating* (FR) based on how other nodes have rated the same friend node, and *net rating* (NR) which is a combination of DR and FR. In FACES, new routes are requested on demand but challenges, friend sharing and rating are periodic processes which renders FACES a hybrid routing protocol.

2.5. Summary

This Chapter has presented an overview of the most common MANET routing protocols, routing attacks, and a critical evaluation of the well-known secure MANET routing protocols. Originally routing protocols were designed without taking security into account, so secure routing protocols have tended to be introduced as extensions to existing protocols. These are mainly divided into three categories; cryptography based, reputation based and their combination. All the reviewed routing protocols and the secure extensions are

summarised in Table 2.1 while their routing attack protection capabilities are comparatively evaluated in Table 2.2.

Table 2.1: Well-known MANET routing protocols and their secure extensions.

Routing protocol Type	Routing protocol base	Secure routing protocol		
		Cryptography based	Reputation based	Cryptography & reputation based
Reactive	AODV	SAODV SAR	CORE FrAODV	TAODV
	DSR	Ariadne	CONFIDANT TSR	
	AODV/DSR			SRAC
	-	ARAN		
Proactive	DSDV	SEAD		
	OLSR			SLSP
Hybrid	ZRP	SRP		
	-			FACES

Table 2.2: Comparative evaluation of the most well-known secure routing protocols and their key protection attributes.

	Protocol	Provides protection against attack:						
		Modification	Impersonation	Fabrication	Rushing	Wormhole	Replay	Selfish
Cryptography	SAODV	Yes	Yes	Yes	No	No	Yes	No
	ARIADNE	Yes	Yes	Yes	Yes	Yes	Yes	No
	ARAN	Yes	Yes	Yes	Yes	Partially	Yes	No
	SAR	Yes	Yes	Yes	Yes	Partially	Yes	No
	SEAD	Partially	Yes	Yes	No	No	No	No
	SRP	Yes	Yes	Yes	No	No	Yes	No
Reput.	CONFIDANT	Yes	No	No	No	No	No	Yes
	CORE	Yes	No	No	No	No	No	Yes
	FrAODV	Yes	No	No	No	No	No	Yes
Crypt. & Reput.	TSR	Yes	No	No	No	No	No	Yes
	SLSP	Yes	Yes	Yes	Yes	Partially	Yes	No
	SRAC	Yes	Yes	No	Yes	Partially	Yes	Yes
	TAODV	Yes	Yes	Yes	Yes	Partially	Yes	Yes
	FACES	Yes	No	No	No	No	No	Yes

Secure routing protocols based on cryptography, typically require each node in the network to cryptographically authenticate itself. For example Ariadne, ARAN, and SAR provide protection against modification, fabrication, impersonation, rushing and PM wormhole attacks, where malicious nodes need to read and modify routing packets for the attack to succeed. However, HM wormholes cannot be detected using cryptography since they do not modify any routing packets. Cryptography-based protocols also assume that none of the

authenticated nodes are malicious. In a MANET environment where it is straightforward to discern legitimate users/nodes from others, such as in a military or small company MANET, trust relations are easy to set up and security measures based on cryptography are correspondingly straightforward to realise.

In contrast, in a dynamic large-scale MANET where a multitude of nodes are arbitrarily joining and leaving the network, it is impractical to predict whether a node will act maliciously or legitimately without having prior knowledge of its behaviour. Another drawback of using cryptography is that trusted third parties are needed, including certification authorities to establish trust in certificates and centralised key distribution mechanisms to deliver shared secret keys to nodes which is not congruent with the infrastructure-less nature of MANETs and are impractical in highly dynamic topologies. Furthermore, on hardware restricted devices, such as small sensors, cryptography cause a high computational overhead. Notable in the Table 2.2 evaluation is that it is assumed that selfish nodes are legitimate and thus cryptography based secure routing protocols cannot detect them.

An alternative approach to building up trust to other nodes is based on their reputation. To detect selfish nodes and modification attacks the communication activity of each node can be monitored as proposed in CONFIDANT, CORE, and FrAODV. If it is identified that a certain neighbour node is not forwarding routing packets or it falsely modifies routing packets, then its trust level will be decreased and omitted during future routing discovery procedures. However, these protocols have no mechanisms for authenticating nodes or routing messages and thus they are vulnerable to impersonation, fabrication, rushing and replay attacks where malicious nodes neither drop nor falsely modify routing packets. To address this limitation, several secure routing protocols which are a combination of cryptography and reputation have been proposed, such as TSR, SLSP, SRAC, TAODV, and

FACES. Another challenge to the real-world adoption of reputation-based mechanisms is that they impose extra network overheads, as they typically involve MANET nodes operating in promiscuous mode. A promiscuous node is one which analyses all received packets, including those addressed to other nodes, in order to monitor the behaviour of its neighbours.

A common limitation of all evaluated secure MANET routing protocols is that they do not provide complete protection from wormhole attacks. All protocols requiring authentication of each intermediate node, such as ARAN, SAR, SLSP, SRAC and TAODV, prevent the formation of a PM wormhole by assuming an authenticated node is not malicious. In contrast, HM wormholes are not detected based on encryption since these do not need to either read or modify routing packets. The Ariadne protocol exceptionally also detects HM wormholes by including a timestamp in the routing packets to measure the time-of-flight of the routing packets between two neighbours, but it impractically requires tightly synchronized clocks.

These observations provided the motivation for doing further research into wormhole attack detection in MANETs. The research area, has in recent years been particularly topical due to the severity and corresponding challenges in accurately detecting wormhole attacks and many security extensions to routing protocols have emerged which directly focus on wormhole attack detection. In the next Chapter, wormhole attacks and their impact on MANET routing security will be examined in detail, with a rigorous literature review on wormhole detection strategies being presented.

3. WORMHOLE ATTACK DETECTION: A LITERATURE REVIEW

3.1. Introduction

From a MANET perspective, wormholes are especially difficult to detect for two key reasons. Firstly there is the latent variability in the environment in terms of the number of users, their locations, and the applications and services they are executing. A MANET can operate as either a closed network, where a legitimate node may easily be separated from an unauthorized node, or alternatively as a highly dynamic network exhibiting considerable intermittent nodal connectivity making it very challenging to distinguish malicious from legitimate nodes. Furthermore, network devices can vary from small energy constrained computing devices with limited hardware capability to powerful personal computers. The second reason is the diversity of feasible wormhole attacks, i.e., *participation mode* (PM), *hidden mode* (HM), *in-band* (I-B) and *out-of-band* (O-B) channels. Each wormhole type has its distinct characteristic providing the opportunity to launch the attack in many different modes, with each mode imposing its own set of challenges for any detection mechanism. In addition, cognizance of the incidences of erroneous wormhole identification, so called *false positive* (FP) must also be considered in any proposed detection paradigm.

During the last decade, a lot of research has focused on wormhole attack detection, on the distinctive features of an attack, and on the behaviour of both the network and specific nodes when a MANET is under attack (Gupta & Gupta, 2014; Khan et al., 2013). In the next Section, state-of-the-art wormhole detection methods are reviewed and critically evaluated.

3.2. Classification of Wormhole Detection Proposals

Typical features that have been utilized in wormhole detection schemes are RSSI, *number of neighbours*, *network visualization*, *frequency of node/link appearances in routes*, *location information* and *packet delay*. Some schemes also utilize a combination of the above

mentioned features for achieving more robust wormhole attack detection. The appropriateness of these individual features for detecting the different wormhole variants and examples of wormhole detection methods based on these features will now be critiqued.

3.2.1. Received Signal Strength Indicator (RSSI)

In Jain et al. (2012) a scheme based on wireless channel characteristics is proposed for detecting and avoiding wormhole attacks. The basis is that when two nodes send data frames to each other during a short time period, the frames will be received with similar RSSI values and these values can be correlated with the communication partner. Correspondingly, when a node communicates with several artificial neighbours through the same HM wormhole link, then the RSSI values for the frames received from all neighbours will be similar and can thus not be correlated with the neighbours. This observation can be utilized for wormhole attack detection either during the neighbour/route discovery phase or during the whole duration of transmission of data packets between two nodes to build up a trust metric. In order to achieve optimal wormhole attack detection by analysing RSSI, multiple data frame exchanges are required so the trust metric method is significantly more robust. Some assumptions concerning the wireless channel must be upheld however, namely that it is symmetric between each node pair, and while this may be reasonable for a static network or in a network where there is low node mobility, for a dynamic MANET it is not a viable solution.

A similar protocol, called *secure channel reciprocity-based wormhole detection* (SCREWED) is proposed in Krentz & Wunder (2014) to detect HM wormholes in *IPv6 over low-power wireless personal area networks*. In SCREWED the assumption for symmetric RSSI is relaxed by using alternative channel reciprocity metric. SCREWED improves wormhole and reduces false positive detection compared with Jain et al. (2012) by using channel hopping, randomized transmission powers, message integrity codes and a special

replay protection mechanism. However, neither of these two protocols is capable of detecting PM wormholes since these always appear in a network as legitimate neighbours and therefore they are not viable for fulfilling the overarching research question.

3.2.2. Neighbour Count

A *statistical wormhole apprehension using neighbours* (SWAN) (Song et al., 2012) algorithm has been proposed which is based on the observation that the number of 1-hop neighbours is significantly higher for a node placed in a region close to a HM wormhole than when placed in a wormhole-free region. When a node moves into a wormhole infected region it experiences a rapid increase in the number of neighbours, and this irregularity in the number of neighbour nodes is detected using an outlier detection algorithm. This approach however, is not able to detect PM wormholes since such wormholes do not affect the number of 1-hop neighbours. Furthermore, SWAN only identifies a wormhole infected region and not the exact infected route or the malicious nodes.

3.2.3. Network Visualization

The main idea of network visualization based wormhole detection schemes is to collect connectivity information from each node in the network, using for example, signal strength or neighbour information, and then to visually recreate the network to identify anomalies in its structure. Since the whole network can be examined, and not only the neighbourhood of a specific node, both PM and HM wormholes are detected independently of the connectivity link used, i.e. I-B or O-B. Some of these schemes will now be critically evaluated.

Multi-dimensional Scaling Visualization of Wormhole (MDS-VOW) (Wang & Bhargava, 2004)

MDS-VOW is a centralized wormhole defence mechanism proposed for sensor networks. All network nodes estimate the distances to their neighbours based on signal strengths, and these are all sent to a centralized controller which calculates the distances between all nodes

in the network using Dijkstra's algorithm. The controller then uses multi-dimensional scaling to graphically reconstruct the whole network. If the surface of the reconstructed network is flat, it indicates that no wormhole exists. If the surface between two nodes is warped, then a wormhole is suspected to exist. However the need for a centralized controller is unrealistic because this compromises the essential self-configuring and infrastructure-less features of a MANET.

Topological Detection (Dong et al., 2011)

This approach is similar to MDS-VOW but includes the enhancement that no centralized controller is needed. Instead, wormhole detection is based on a distributed approach completely relying on network connectivity information. Network nodes are basically exchanging neighbour connectivity information between each other and are then able to find anomalies in the network topology by analysing a connectivity graph. However, this scheme places a high overhead on network nodes since connectivity information must be periodically exchanged.

WormPlanar (Lu et al., 2013)

WormPlanar is a topology based wormhole detection using planarization to reflect essential changes in the network topology caused by wormholes based on only local connectivity information. Each node gathers *k-hop* neighbourhood information before applying a planarization algorithm (Dong et al., 2013) on the neighbourhood subgraph of each node. The authors have observed through simulations that $k = 5$ is sufficient to achieve good wormhole detection results. Planarization simply means redrawing the neighbourhood sub-graph in such a way that when drawing a line between each connected node pair, none of the lines intersect each other. In Dong et al. (2013) it has been proven that a connected planar topology can be extracted from a normal network sub-graph by using the planarization algorithm while the algorithm will fail when a wormhole attack is present in the sub-graph.

Under normal circumstances the neighbourhood of a node would expand continuously around it, while if it is a wormhole node or close to an end of a wormhole, its neighbourhood would expand at the two ends of the wormhole link. Each node that fails to obtain a planar topology is considered as a suspect wormhole node. Finally, possible FP detections are removed by performing a refinement process where all suspected nodes are filtered by two simple wormhole attack conditions. For instance, legitimate nodes located close to one of the ends of the wormhole link will not pass the planarity test and so are falsely suspected as being wormhole nodes.

WormPlanar provides a reasonable detection performance for all types of wormholes, though it is highly dependent on the node density in the network. For example, the requirement for 100% wormhole detection in a randomly deployed network is that the average amount of 1-hop neighbours per node is at least 10 (Lu et al., 2013). So, if a wormhole link is the only connection link between two portions of a MANET, then the detection algorithms will fail.

3.2.4. Frequency of Node Appearances in Routes

These wormhole detection approaches are based on the fact that wormhole nodes typically attract significantly more network traffic than legitimate nodes. Therefore, wormhole nodes appear more frequently in routing tables than legitimate nodes. Examples of such wormhole detection schemes are *statistical analysis of multipath* (SAM) (Qian et al., 2005), *wormhole avoidance routing protocol* (WARP) (Su, 2010), and the wormhole avoidance scheme based on route participation cost (Azer et al., 2009). These will be now be surveyed.

Statistical Analysis of Multipath (SAM) (Qian et al., 2005)

SAM detects wormhole attacks in multipath routing protocols such as DSR. The relative frequency of each link that appears in all obtained routes for one route discovery is

calculated, and the link with the highest relative frequency identified as a wormhole link.

Wormhole Avoidance Routing Protocol (WARP) (Su, 2010)

This is an AODV-based protocol where legitimate nodes are able to discover wormhole nodes with abnormal path attractions. If the wormhole node appears in more routes than a certain threshold value in the neighbour's routing table, then the wormhole node will be avoided in future communication. Hence, the wormhole node will gradually become isolated by neighbouring nodes and eventually be quarantined by the full network.

Wormhole Avoidance based on Route Participation Cost Analysis (Azer et al., 2009)

This is a wormhole prevention extension to AODV where each node is assigned a cost according to the number of times it has participated in routing for a certain destination. The route with the minimum cost is then always chosen during route discovery. As a result, a wormhole node is unable to attract traffic all the time. This solution, however, does not detect either the wormhole route or the malicious nodes and it also increases the delay compared to the default AODV protocol.

A common and crucial limitation considering their potentials for answering the main research question is that these schemes can only detect PM wormholes because HM wormhole nodes never appear in any obtained route. Furthermore, they rely upon the assumption that a particular wormhole node always appears in the network with the same identity. If a specific malicious node would for example alternate between several different identities it would be registered in routing tables with many different identities and thus a high frequency of routing participation of that node would not so easily be discovered.

3.2.5. Hop Count

Wormhole attacks typically offer a route with a lower *hop count* (HC) than legitimate routes and therefore they attract a high amount of network traffic. This feature is utilized in *Multi*

hop-count analysis (MHA) (Jen et al., 2009) which is a wormhole avoidance scheme designed as an extension to AODV. As a result of basic AODV route discovery, the route with smallest HC is obtained. MHA introduces a RREP number limit ($RREP_{lim}$) variable defining the number of unique routes that need to be obtained during the route discovery process. If $RREP_{lim} > 1$, the source node stores the intermediate nodes of the discovered route in a so-called *graylist* which is distributed to all other nodes in the network along with a second route discovery. An intermediate node receiving a *graylist* broadcast message checks whether the previous hop is in the *graylist*. If it is, then the broadcast message is dropped. If not, the message will be treated as a normal AODV RREQ message. As a result of *graylist* broadcast, the source node obtains an alternative route to the destination, consisting of other intermediate nodes than the ones in the previously obtained route. The *graylist* broadcast procedure is repeated as long as the number of discovered routes is less than the $RREP_{lim}$ value. At the end of the *graylist* broadcast procedure, the HC values of the obtained routes are compared and a route with a significantly lower HC than other obtained routes will be avoided during data communications.

In the context of the overarching research question defined in Chapter 1, MHA is an attractive solution since it is computationally lightweight, only the source node needs to execute the detection algorithm, no additional hardware is required and it is independent of the wormhole type. As a consequence, MHA will be used as one of the comparators in the critical evaluation of the new wormhole detection framework presented in this thesis. The major weakness of MHA is that it relies on the fact that the wormhole route will always have the smallest HC which is not necessarily true in a real world network topology, where source and the destination nodes are not always located close to each end of the wormhole link. The example in Figure 3.1 illustrates this problem where A is the source node, D is the destination node, while E and F form a PM O-B wormhole.

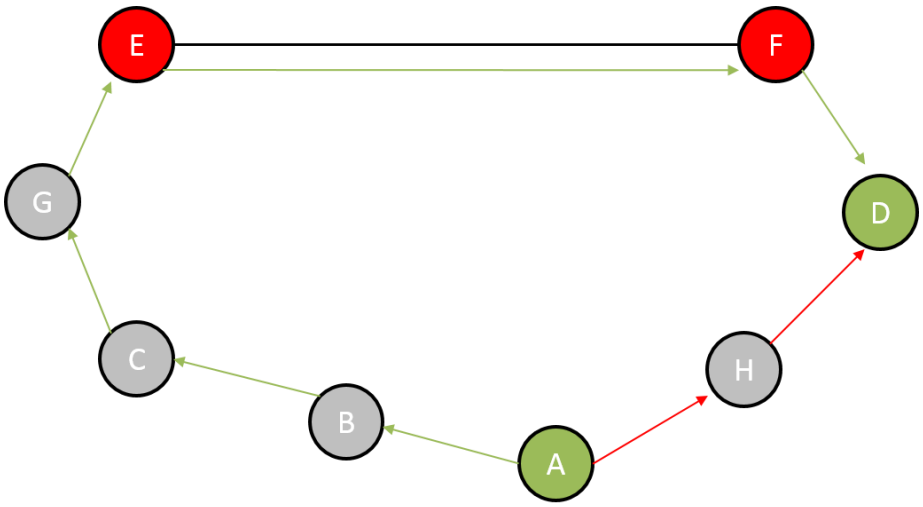

Figure 3.1: MANET topology example including source node A and destination node D where MHA fails to detect a PM O-B wormhole formed by nodes E and F.

In this case, the HC of the shortest route is 2 (A→H→D), while the alternative route HC = 6 (A→B→C→G→E→F→D) results in MHA preventing packets from being routed through H since that route has a significantly lower HC than the wormhole infected route. Therefore, in a real world MANET where nodes are uniformly distributed, MHA causes many FP detections.

3.2.6. Node Location

Since the purpose of a wormhole attack is to create the illusion that two distant nodes or network regions are neighbours it is natural to counter such an attack by analysing the geographical locations of the nodes in the network. In this Section, a review of some wormhole detection schemes based on location information is presented.

Geographical Leash (Hu et al., 2003)

A Geographical leash ensures that the recipient of a packet is within a certain distance from the sender. It is based on the assumption that all nodes know their own locations and have "loosely" synchronized clocks. The sending node adds to every packet a leash, including its geographical position and the time when the packet was sent. The node that receives the packet then compares the leash values with its own geographical position and time of

reception. If the nodes are located further away than a threshold (maximum radio range between two nodes) a wormhole is suspected to exist between the sender and receiver. This type of geographical leash is only effective however for HM wormholes since the distance is only validated between two neighbours, and not over several hops as would be required for PM wormhole detection.

Route Packet Leash (Wang et al., 2006)

A node location-based approach similar to geographical leashes is proposed to detect anomalies in neighbour relations. Each node forwarding a RREQ inserts a time stamp and its location information into the routing packet. This information is secured with a **MAC**. When the destination node receives a RREQ it checks the positions of all intermediate nodes on the route and if two nodes are out of communication range from each other, then a wormhole is suspected. This mechanism is capable of detecting all types of wormholes (HM, PM, I-B, and O-B) with the underlying assumptions that the source and destination have a trusted relationship, that all intermediate nodes have access to their location information, and that node clocks are "loosely" synchronized.

Simple and Efficient End-to-End Protocol (SEEEP) (Gupta & Khurana, 2008) and First End-to-End Protocol with Variable Ranges (FEEPVR) (Khurana & Gupta, 2008)

Two other approaches which adopt the same principle are SEEEP and FEEPVR. In these protocols a route is suspected to be under wormhole attack if the route HC is small in relation to the route distance and the node radio ranges. SEEEP and FEEPVR also provide defence against PM wormhole nodes, which present false HC values, by requiring each intermediate node to include its ID and **MAC** (calculated by a secret key shared by itself and the destination) to a *traversed hop list* (THL). However, this requires every node to share a secret key with every other node in the network, which makes them impractical for dynamic

MANET environments. To check whether every node provides correct location information, the destination node checks from the received THL whether every two consecutive intermediate nodes are in the communication range of each other. All checks are performed by the destination node.

A Range-free Localization Scheme (García-Otero & Población-Hernández, 2012)

This scheme is proposed for detecting wormhole attacks in WSNs where only certain MANET nodes are required to know their exact locations. This scheme can be integrated within any WSN localization protocol and can operate either during the localization procedure or be used as validating already estimated positions after the localization process. An arbitrary node *i* can estimate its position with the help of anchor nodes and RSSI analysis of their wireless signals. An anchor node is a device having exact location information and is directly connected to node *i*. It must also be in direct communication range with at least 3 other anchor nodes and be able to obtain RSSI values for these connection links to estimate its position. By estimating its position, each node is able to detect HM wormholes trying to make two distant regions of a WSN appear adjacent. The authors showed through simulations that the proposed scheme is effective under good channel conditions, though the wormhole detection performance degrades in the presence of shadowing effects that occur in non-LOS environments.

Detection methods based on location information are effective on all types of wormholes as long as each node has a positioning device and is able to provide accurate location information. However, the use of a positioning device, such as *global positioning system* (GPS), is impractical, especially in WSNs consisting of hardware restricted computing devices. Even in a MANET consisting of more powerful device like smart phones or tablet computers, the GPS device leads to high battery consumption and if the MANET is located indoors, GPS devices are unable to receive accurate position information. Even though the

range-free localisation scheme slightly relaxes the assumption that each node is aware of its exact location, it still requires in practice that the majority of the nodes are located outdoors and equipped with positioning devices. For these reasons, location based detection schemes have not been considered for further study in this thesis.

3.2.7. Packet Delay

The rationale behind packet delay based countermeasures is to estimate either the average distance per hop or the distance between two neighbour nodes on a route by measuring the delay of transmitting a packet (typically routing packet) to another node. A route having a large delay in relation to the HC or a hop delay being significantly larger than others can indicate a wormhole. There now follows a critical evaluation of some existing packet delay countermeasures.

Temporal Packet Leash (Hu et al., 2003)

The basic idea of a temporal packet leash is to define an upper limit on the lifetime of a packet to restrict the maximum distance D_{MAX} it can travel. When a node sends a packet at local time t_{loc1} it sets the packet expiration time to $t_{exp} = t_{loc1} + \frac{D_{MAX}}{S} - \Delta$ where S is the propagation speed of the wireless signal (i.e. the speed of light = $3 \cdot 10^8$ *m/s*) and Δ is the maximum time synchronization error. A receiver at which the packet arrives at local time t_{loc2} suspects that a wormhole exists between the sender and the receiver and drops the packet if $t_{exp} > t_{loc2}$. The t_{exp} value must be protected to prevent it from being altered by a wormhole node with **MACs**, digital signatures and hash chains being proposed for this purpose.

While the temporal packet leash is an effective method for detecting HM wormholes, it cannot detect PM wormholes because these appear in routes as legitimate neighbours and therefore they can easily ignore the packet leashes. Ariadne (Hu, 2002) on the other hand (see Section 2.4.1) uses the TIK protocol for implementing temporal packet leashes for

detecting HM wormholes and uses symmetric keys for authenticating all intermediate nodes to prevent PM wormholes. Another limitation of packet leashes is that they require tight clock synchronization, which is an impractical restriction in a heterogeneous MANET.

Timing-based Countermeasure (Khabbazian et al., 2009)

The timing-based countermeasure eliminates the need of clock synchronization in temporal packet leashes. Each node in the network validates its neighbours by an exchange of two signed messages as illustrated in Figure 3.2.

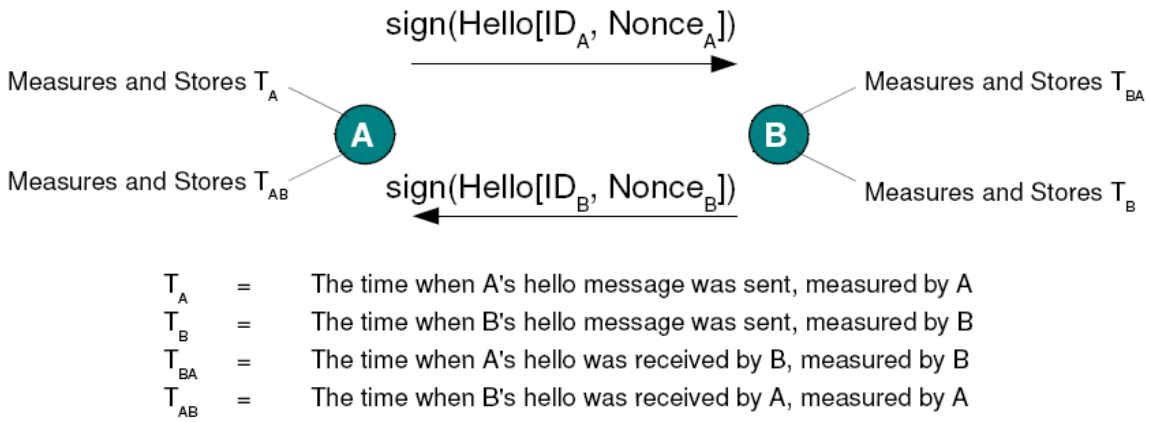

Figure 3.2: Exchange of Hello messages between nodes A and B.

Suppose node A wants to verify that node B is its neighbour. Node A sends a Hello message (broadcasted to all neighbours), to which B responds with its own Hello message. Both nodes then send a Follow-Up message after receiving a Hello message (see Figure 3.3). When node A receives the Follow-Up message from node B it firstly verifies the signature of B and checks if the received nonce is the same as the one A sent in its Hello message. If both verifications are successful, node A can accept node B as neighbour provided $\frac{(t_{AB}-t_A)-(t_B-t_{BA})}{2} * S \leq R$ where R is the maximum node radio range. This solution though is similar to temporal packet leashes, in only being effective against HM wormholes since PM wormhole nodes can easily ignore the neighbour validation process. Additionally, since

every node in the network is required to execute a signature and a signature verification operation for every routing packet it both receives and forwards. This imposes a significant high load upon the network devices, many of which will have low processing capacity and be energy constrained.

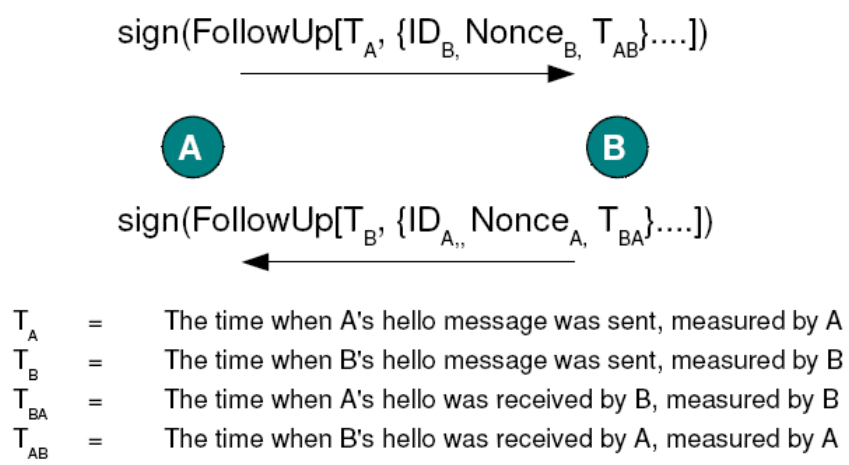

Figure 3.3: Exchange of Follow-Up messages between nodes A and B.

However, the underlying concept of time measurement, attractive due to its accuracy and independence of synchronized clocks, provided the motivation to investigate in greater depth, how this concept could be extended to detect PM wormholes. This partially formed the basis of the new TTHCA wormhole detection model which will be introduced in Chapter 5.

Two-hop Neighbour Discovery (Lee et al., 2008)

This is a packet delay and cryptography based scheme proposed to detect both HM and PM wormholes. Each node must maintain a list of valid 1-hop and 2-hop neighbours and set up a session key with each of them. Neighbours are validated by broadcasting control messages over 2 hops. All 1-hop and 2-hop neighbours responding to the broadcast message within a certain time interval are considered valid. Every node sending or forwarding routing messages must include its identity and a **MAC** in the message. A node receiving a routing

message checks whether it was sent from a valid 1-hop or 2-hop neighbour by validating the **MAC**. If a routing message with an invalid **MAC** is received a wormhole attack is suspected.

This scheme is more effective than temporal packet leashes and the timing-based countermeasure described previously, since it can also detect PM wormholes, but involves heavy cryptographic operations. Moreover, to continually monitor both 1-hop and 2-hop neighbours is a time consuming process, especially if the network topology is highly dynamic. Also a PM O-B wormhole cannot be effectively detected by solely analysing the time delay of the exchange of neighbour broadcast and acknowledge messages, because the time delay on such a wormhole link is negligibly small compared to the variation in packet processing delays on the 1-hop and 2-hop neighbours.

Delay per Hop Indicator (DelPHI) (Chiu & Lui, 2006)

The purpose of the DelPHI technique is to find all available routes between a source and a destination by using a modified AODV route discovery procedure. During this procedure, the RTT and HC of each route are firstly measured and then the *delay per hop* (DPH) calculated as $DPH_I = \frac{RTT_I}{2HC_I}$. A wormhole route is identified based on the assumption that a route traversing a tunnelled wormhole link has a significantly higher DPH than a normal route. Thus, the DPH values of all routes are ranked in descending order and a wormhole suspected if any $(DPH_{I+1} - DPH_I) > T$, where T is the maximum permissible difference between two adjacent DPH values.

DelPHI is an attractive detection solution since it is lightweight in terms of both computational complexity and network load, and it is capable of detecting both HM and PM wormhole nodes, provided the wormhole link is established using an I-B channel. However, O-B wormholes cannot be effectively detected by analysing DPH, because the time delay on such a wormhole link is negligibly small compared to the variation in packet processing

delays on intermediate nodes. Furthermore, as shown in Chiu & Lui (2006), the wormhole link must be up to 8 hops in most scenarios before 100% detection is achieved. Despite these limitations, DelPHI helped frame the motivation behind the development of TTHCA to fulfil *Objective 1*, and is consistently applied as a comparator in the critical analysis of the performance of TTHCA in Chapter 5.

Wormhole Attack Prevention (WAP) (Choi et al., 2008)

This is a more advanced version of DelPHI and is designed to not only detect wormhole routes but also prevent malicious nodes reappearing in routes. Every node, initiating or forwarding a RREQ, executes a neighbour node monitoring procedure to detect HM wormholes. As soon as a node sends a RREQ packet it calculates a *wormhole prevention timer* (WPT) as $WPT = \frac{2R}{S}$ and waits for the retransmission of the neighbour node. WPT is basically a value defining the maximum time a packet is allowed to travel from the sender node to a neighbour node and back to the sender. If the time from sending the RREQ until overhearing the retransmission of the RREQ message by the neighbour is higher than WPT, a HM wormhole link can be considered to exist between the sender and the neighbour node (which in this case is a fake neighbour). This wormhole detection procedure is performed by every node sending or forwarding a RREQ during route discovery. To detect PM wormholes, WAP uses a technique similar to DelPHI by calculating a DPH value for every available route to a destination. If *DPH > WPT* for a specific route, the route is suspected to include a PM wormhole link. This analysis is not only performed at the source, as in DelPHI, but on every intermediate node receiving a RREP. Thus, if DPH at node *#i > WPT* then nodes *#i+1* and *#i+2* are pinpointed as PM wormhole nodes and placed in a blacklist. Nodes on the blacklist are ignored in future route discovery procedures and hence the PM wormhole nodes are prevented from reappearing in routes.

Transmission Time based Mechanism (TTM) (Tran et al., 2007)

TTM is a RTT-based wormhole detection scheme, similar to WAP and DelPHI, which measures and analyses RTT between each successive node ($RTT_{i,i+1}$). The source and each intermediate node measures RTT between itself and the destination (RTT_i), i.e. the time from sending/forwarding a RREQ ($\{T_{RREQs}\}_i$) until receiving the corresponding RREP ($\{T_{RREPr}\}_i$). Each RTT_i value ($RTT_i = \{T_{RREPr}\}_i - \{T_{RREQs}\}_i$) is then delivered to the source node in an additional parameter in the AODV RREP packet. Based on the RTT_i values received in the RREP, the source calculates the RTT between each two successive nodes on the path as $RTT_{i,i+1} = RTT_i - RTT_{i+1}$. A wormhole is detected using the assumption that $RTT_{i,i+1}$ is significantly higher between two successive nodes connected to a wormhole link than for any legitimate hop. The threshold for the maximum permissible $RTT_{i,i+1}$ is empirically estimated via simulations.

Wormhole Attack Detection Using Hop Latency and Adjoining Node Analysis (WAD-HLA) (Vandana & Devaraj, 2013)

DelPHI, WAP and TTM have all the recurring limitation that packet processing time variations on nodes must be small to both achieve 100% wormhole detection and avoid unreasonably high FP detections. WAD-HLA attempts to decrease the FP detections by combining hop RTT analysis with adjoining node analysis. Firstly, the RTT for each successive hop is measured and calculated in a similar manner to that in TTM. If any hop RTT is suspiciously high, then the route is considered as a potential wormhole infected route and the two successive nodes causing the high RTT value are considered as suspected wormhole nodes. A confirmation phase is then performed to ensure that the route really is wormhole infected by verifying if any adjoining node exists between the suspected wormhole nodes. If a node is identified along the path between suspect wormhole nodes, then a wormhole is confirmed. WAD-HLA still relies solely on hop RTT analysis for

wormhole detection however, and so exhibits the same limitations as DelPHI, WAP, and TTM.

Analytical Hierarchy Process Methodology (Shi et al., 2013)

This approach against wormhole attacks uses special nodes, called *local most trustable* (LMT) nodes, located close to the source and destination to perform the detection. The neighbours of the source and the destination with the largest weight values are elected as the LMT nodes. Weight values are calculated based on the *relative stability*, *credit value* and *reciprocal of forward rate*, where *relative stability* is evaluated based on the change rate of neighbors, the *credit value* is based on packet transmission behavior, and *the reciprocal of forward rate* is evaluated based on packet forwarding rate. Once the LMT nodes are elected for a specific source and destination node they perform the wormhole countermeasures for a route between that particular source and destination. A potential wormhole on a requested route is detected by comparing the HC value extracted from the RREP packet with a minimum HC value which is estimated based on the RTT and the mean transmission range of all nodes. The RTT of the route is measured by exchanging a hello request and reply message between the source LMT node and the destination LMT node after the source has received a RREP message. The route is considered wormhole infected if the route HC is less than the estimated minimum HC value. The motivation for introducing LMT nodes for wormhole detection, instead of using the source and the destination nodes, as in most other proposals is that the source and destination nodes cannot always be considered trustworthy. However, the process of calculating weight values and electing LMT nodes leads to a significant network overhead, especially if the topology is dynamic.

Neighbour Probe Acknowledge (NPA) (Zhou et al., 2012)

NPA is an alternative RTT-based approach aimed at improving the wormhole detection performance of related methods by analysing the standard deviation of RTT (*stdev(RTT)*)

instead of RTT. The authors have observed through theoretical analysis and experimental results that this is a significantly more effective metric for identifying the existence of a wormhole than RTT. NPA is designed for wireless Mesh networks and is triggered when a node detects a change in the network topology. RTT values are obtained locally by each node exchanging probe messages with its neighbours *n* times. A large *stdev(RTT)* indicates that two neighbours are connected through a wormhole. The performance of NPA has been evaluated in a real test bed consisting of a HM wormhole with an O-B link through a network cable and the results reveal that NPA performs significantly better than DelPHI both in terms of wormhole and FP detection. However, since the RTT is only measured on a neighbourhood basis, PM wormholes cannot be detected. NPA also tends to increase the network overheads, especially in highly dynamic networks because of the multiple exchanges of probe messages (typically 50) for each change in the topology.

Modified TTM (in this thesis it will be referred to as M-TTM) (Qazi et al., 2013)

M-TTM is proposed to overcome the limitations of RTT-based methods. In addition to each node measuring hop RTT ($RTT_{i,i+1}$) just as in TTM, each node also estimates the *expected RTT* to its next hop, i.e. the sum of the RREQ and RREP packet processing times measured at the next hop and the maximum *propagation delay* (PD_{MAX}). $RTT_{i,i+1}$ is then compared with the *estimated* $RTT_{i,i+1}$ and if it is significantly higher, a wormhole is suspected. M-TTM provides more robust wormhole attack detection than TTM and other RTT-based schemes, since packet processing times are taken into account in the RTT measurements. However, under certain conditions M-TTM has a number of limitations. Each node along a route must add four different timestamps to every routing packet to reflect the specific times incurred in receiving and forwarding RREQ and RREP packets. The assumptions underpinning how the *estimated* $RTT_{i,i+1}$ is determined are also unrealistic, since PD_{MAX} is presumed to be $1\mu s$ which correlates to a distance of about 300 m. In a real MANET, the PD_{MAX} of a node will be dependent on both its hardware and surroundings, since in a LOS link PD_{MAX} will be much

higher than when there are obstacles between nodes. Furthermore, applying a fixed 2 ms threshold for the maximum difference between the measured and *expected RTT* values means that not all wormhole types can be detected. If the MANET has a PM O-B wormhole for instance, where the *propagation delay* (PD) between the malicious nodes is the only extra delay incurred, $RTT_{i,i+1} > expected\ RTT_{i,i+1}$ already indicates the presence of a wormhole since $RTT_{i,i+1}$ excluding packet processing time at node #$i+1$ cannot be $> 2PD_{MAX}$ if nodes #i and #$i+1$ are legitimate.

Despite the above mentioned limitations, the underlying concept of analysing the packet delay for each hop makes this solution attractive since it provides the base for more accurate wormhole attack detection compared to those analysing the average delay per HC, such as DelPHI and TTHCA. Thus, this partially inspired the base for the new extended version of TTHCA, i.e. the TTpHA wormhole detection model which will be introduced in Chapter 6 for fulfilling research *Objective 2*. M-TTM is thus also applied as a comparator in the critical analysis of the performance of TTpHA.

3.2.8. Wormhole Detection Proposals Combining Multiple Features

Some detection proposals analyse multiple wormhole related features in order to achieve more accurate detection performance. They typically operate in a similar manner to IDS and constantly monitor the network behaviour, rather than concentrating on wormhole detection during the route discovery process. A critical review of wormhole detection schemes that fall into this category is now presented.

Decentralized Intrusion Detection Scheme (Azer et al., 2010)

In this scheme, network monitors are measuring suspected parameters for a wormhole attack, such as the speed of arrival per hop of packets, transmission power of nodes, and the actual locations of a source and destination node. These parameters are then used by each node to

make a central decision about the behaviour of network nodes according to a chosen decision scheme. The AODV protocol is modified to allow route selection based on nodes' opinions of each other instead of the lowest HC. This scheme is attractive to MANETs since the actual wormhole detection method is simple and incurs no computational cost. The disadvantage is that it significantly increases the end-to-end delay during routing. Furthermore, the need for network monitors makes the scheme impractical in dynamic MANETs.

Biologically Inspired Artificial Intrusion Detection System (BAIDS) (Sundararajan et al., 2014)

BAIDS is biologically inspired in that it learns normal MANET node behaviour in order to identify abnormal behaviour, mimicking the way the human body is able to respond to foreign antigens. In BAIDS, which is designed as an extension for DSR, AODV and DSDV, each MANET node takes part in the intrusion detection, so no external monitoring nodes are needed. Each node is responsible for detecting malicious behaviour locally and independently, but neighbouring nodes can also work together to examine the network in a broader range. The goal with BAIDS is to not only detect misbehaving nodes but also to prevent them from taking part of the routing once detected.

In BAIDS, each node collects data, such as RREQ packets sent, RREQ packets received, RREP packets sent, RREP packets received, and broken link error packets received. This data must be pre-processed into a certain format before intrusion detection can take place. The algorithm used to detect misbehaving nodes must be trained within a network where there is no malicious behaviour present, before it can distinguish between normal and malicious behaviour. The authors do not explicitly identify the wormhole type yet they claim that they have through simulations proved that BAIDS is able to detect wormholes with high accuracy.

The type of wormhole considered in this context can have a significant impact on the wormhole and FP detection performance as there is a risk that a legitimate node close to the end of a HM wormhole tunnel could be classified as malicious by a node at the other end of the wormhole tunnel if the HM wormhole nodes drop packets. In BAIDS, nodes only monitor packet transmission activity by their neighbours so a wormhole that is only established for MITM attack purposes (instead of disrupting network communications by dropping packets) will go undetected.

Wormhole Detection Scheme based on Projection Pursuit (PP) (Cai et al., 2013)

This is a statistical method that projects high-dimensional data onto low-dimensional subspace in order to find projections that reflect data structures and characteristics of the data. It was observed that the following attribute information needed to be collected for the PP (Jones & Sibson, 1987) based wormhole detection mechanism:

- *Signal strength*: since wormhole nodes often have higher signal strength due to the use of a directional antenna.
- *Throughput:* since wormhole nodes typically attract large portions of network data.
- *Packet loss probability:* as wormhole nodes typically start dropping packets once the wormhole is successfully established.
- *Forwarding delay:* because wormhole nodes may process and forward packets in a slower phase than legitimate nodes since they have a higher load of packets to process.

Network simulator version 2 (*ns-2*) is used to simulate AODV route discovery and data communication of *N* nodes. All four attributes described above are then collected from each network node. Before performing PP, the collected data is homogenised and optimized by a real coding genetic algorithm. Finally, the optimal projection direction is calculated by PP

resulting in security coefficient values for *N* nodes. A high security coefficient value means that the node is trusted and thus not a wormhole node. Correspondingly a low security coefficient value indicates that the node is malicious. PP provides robust wormhole attack detection since it examines several different wormhole features which makes the detection scheme versatile and capable of detecting different types of wormholes. The authors have not though taken HM wormholes into consideration in their performance analysis. HM wormholes can be detected by studying the same data attributes as for PM wormholes but they would lead to FP detections since legitimate neighbours of wormhole nodes would get low security coefficient values. Furthermore, the data collection and pre-processing phases cause a high network overhead.

Pworm (Guoxing et al., 2014)

This real-time passive scheme is proposed for detecting wormholes and locating wormhole nodes in WSNs. The detection and localization algorithm is based on the observation that wormholes attract a large amount of network traffic and after a wormhole link has been successfully set up, the average route HC in the MANET will decrease significantly. Another attribute that has been taken into account in Pworm is that wormhole nodes appear much more frequently in routes than legitimate nodes. Pworm consists of two major parts; *topology collection* during which routing information from the whole network is gathered and *wormhole detection* which is performed by the controller of the network, i.e. the sink node, by analysing changes in the collected routing information. The authors highlight Pworm as a lightweight solution in term of both network overheads and computational complexity since routing information is distributed passively to the sink together with other routing packets (no extra packets are needed) and the calculations needed for wormhole detection and wormhole node localisation are performed only at the sink node, which can be assumed to have adequate computational power. However, while Pworm suits well for static WSNs

it is not applicable in dynamic MANETs where the topology changes continuously and where controller nodes like sink nodes, do not exist.

While these IDS like solutions are able to detect all wormhole types they all share a crucial limitation considering their viability for answering the overarching research question, i.e. the need for constantly monitoring the behaviour of the neighbours for building trust metrics or share connectivity information among the whole network for topology analysis purposes. This typically causes a high network overhead and a fairly static network environment is required.

3.3. Summary

In this Chapter, state-of-the-art wormhole detection solutions have been classified according to their detection strategy and their advantages as well as limitations have been critically analysed. The overall conclusion is that there is a lack of wormhole detection techniques providing accurate detection for all wormhole types without introducing either some impractical assumptions or the imposition of additional hardware, as well as at the same time being lightweight and applicable in different MANET scenarios. The review conclusively shows the lack of wormhole detection/prevention schemes that combine the beneficial features of existing schemes to provide a *hybrid* solution that cannot only be implemented across a wide range of MANET devices (from sensors to notebook computers), but crucially operate in diverse network environments (static, dynamic, small and scalable). Such solutions must incur minimal computational and network overheads, as well as route discovery delays. This provided the setting for the main thesis research question defined in Section 1.3. A summary of wormhole detection strategies and their main limitations in being able to fulfil the main research question is provided in Table 3.1.

Solutions analysing the delay in transmitting a routing/data packet either to the neighbours or over multiple hops and MHA which solely analyses route HC for multiple routes were identified as attractive solutions in the context of the overarching research question and were therefore selected for further study.

Table 3.1: Common wormhole detection strategies and their main limitations.

Analysed feature	Wormhole Type				Main limitations
	HM	PM	I-B	O-B	
RSSI	Yes	No	Yes	Yes	Unable to detect PM wormholes
Neighbour count	Yes	No	Yes	Yes	Only detects an HM wormhole infected region and not the exact infected route or malicious nodes.
Network visualization	Yes	Yes	Yes	Yes	Causes high network overhead and requires high node density.
Frequency of node appearances	No	Yes	Yes	Yes	Only PM wormhole nodes appear in routing tables.
Location information	Yes	Yes	Yes	Yes	Require all or a large part of the network nodes to be aware of their exact geographical positions.
Multiple	Yes	Yes	Yes	Yes	Cause high network overhead and are typically limited to static MANET environments.

The advantages of these solutions are typically that they are low cost in terms of both network and computational complexity, require no extra hardware, are topology independent and easy to implement. The wormhole detection capability and limitations/assumptions of the most attractive solutions within this category are summarized in Table 3.2. However, many of these approaches are based on unrealistic assumptions, such as low variations in packet processing delays due to RTT measurements, or instead impose fixed and impractical thresholds for the wormhole detection algorithm which prohibits them from detecting all wormhole attacks variants under flexible network conditions. MHA on the other hand requires the source and destination node to be located close to the wormhole endpoints.

Table 3.2: Summary of wormhole detection solutions being particularly attractive in the context of the overreaching research question.

Analysed feature	Detection scheme/protocol	Wormhole Type				Limitations/assumptions
		HM	PM	I-B	O-B	
HC	MHA	Yes	Yes	Yes	Yes	Source and destination nodes must be located close to each end of the wormhole link. High FP rate.
Packet delay	Timing-based countermeasure	Yes	No	Yes	Yes	Cryptographic trust relations between neighbouring nodes are required.
	DelPHI	Yes	Yes	Yes	No	Low packet processing time variations on network nodes.
	M-TTM	Yes	Yes	Yes	No	Wormhole detection threshold is based on impractical assumptions.

While packet delay based methods in particular have detection advantages, this provided the motivation to further investigate whether a novel framework can be developed based solely on packet delay analysis, with crucially the assumptions on low radio range variations being relaxed and the wormhole detection performance, significantly improved. Packet delay based solutions have thus inspired the novel contributions of this thesis introduced in Chapters 5 to 7, but before presenting these innovations, the next Chapter discusses the research methodology adopted.

4. RESEARCH METHODOLOGY

4.1. Introduction

In Chapter 1, a new unified wormhole detection framework has been proposed to address the overarching research question. This framework comprises three original inter-linked contributions in the form of the TTHCA, TTpHA and ΔTVE detection algorithms. To critically synthesise and analyse these specific contributions and evaluate their performance in comparison with the existing state-of-the-art detection solutions described in Chapter 3, a suitable research methodology must be adopted. The ideal approach to performance evaluation would be to implement and test the proposed framework in a real MANET environment or testbed. The performance of the framework depends on several factors, amongst them being the wormhole attack type, node measurement accuracy, network size and environment, i.e. obstructed or *line-of-sight* (LOS). As a consequence, a major requirement on the flexibility and scalability of the environment has to be set, in order to ensure rigorous evaluation. Even though a real MANET testbed is in theory a viable option, large scale MANETs are currently not readily available and practical testbeds consisting of hundreds of nodes distributed over a large area are both time consuming and expensive to realise. Consequently, to undertake a critical performance analysis of the new wormhole detection framework, a pragmatic decision was made to initially design and develop a suitably robust MANET simulation environment, while realising that ultimately community expectations will be to apply and assess the framework within a real-world MANET context which will be discussed as a future work option in Chapter 8.

In this Chapter, the simulation environment used for testing and evaluating the new framework's performance is described. Various parameter settings which reflect different MANET environments and scenarios are formally defined, along with the relevant metrics and comparators used for performance evaluation. The strategies employed for validating

the correctness of all the algorithmic software implementations, and the verification of the statistical significance results are also presented. The next Section, provides a description of the adopted research methodology and details of the MANET simulation platform.

4.2. Overview of the Adopted Research Methodology and Simulation Platform

A block diagram of the adopted research methodology is shown in Figure 4.1.

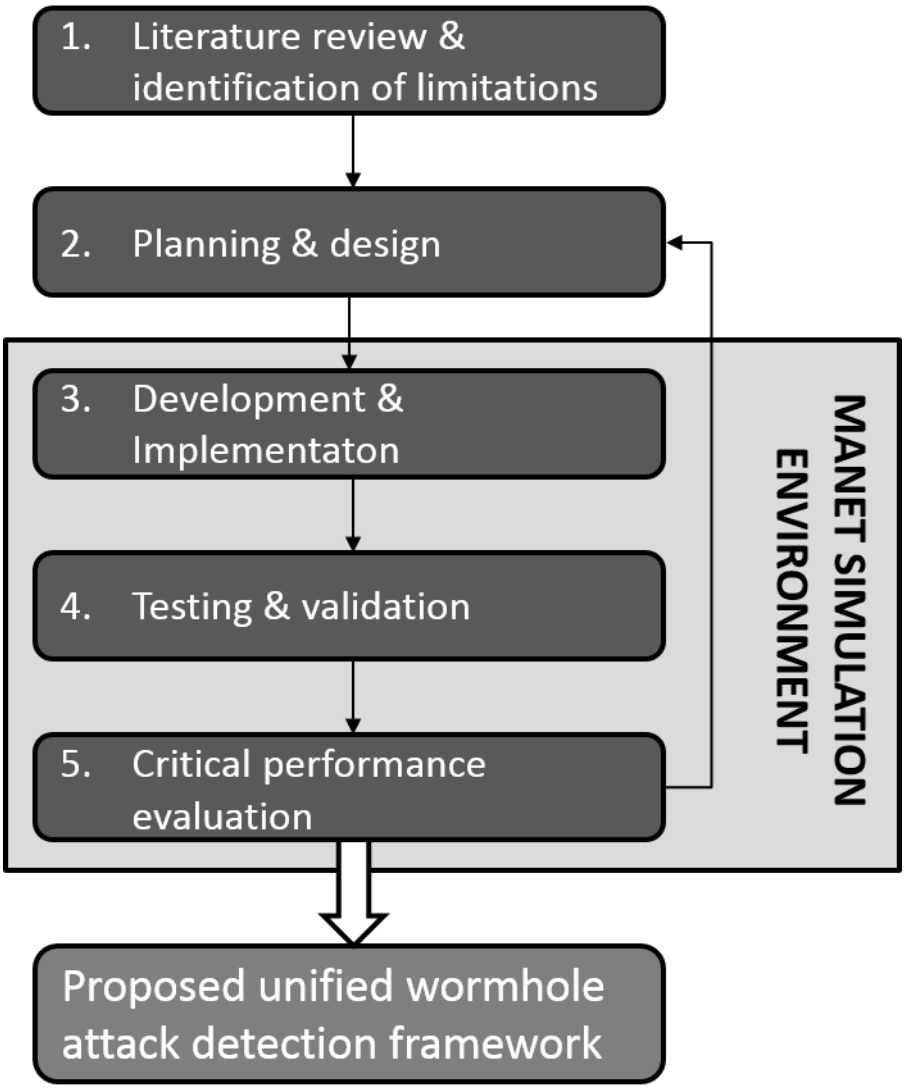

Figure 4.1: A block diagram of the adopted research methodology and its various steps.

The various steps in the methodology are summarised as follows:

1. A thorough literature review on MANET routing security (presented in Chapter 2) was performed and narrowed down to wormhole attack detection (Chapter 3) since wormholes represent one of the most severe threats to MANET routing. Limitations and key assumptions relating to existing state-of-the-art wormhole attack detection solutions have been identified and analysed.

2. *Step 1* provided the motivation and basis for the planning and designing phases of the new unified wormhole attack detection framework by testing and relaxing certain assumptions and where appropriate, addressing their identified limitations.

3. Each algorithmic contribution to the framework was developed and implemented within a dedicated simulation environment (described in Section 4.3) which was used as the standard MANET testbed.

4. Before undertaking a critical performance evaluation of each contribution, the code implementations were validated by correctness checks and by rigorous tests of the functionality. The validation methods used are presented in Section 4.5.

5. The performance of each contribution was critically evaluated for a range of network scenarios, wormhole attack types, and node hardware capabilities using the set of performance metrics which are detailed in Section 4.4. *Steps 2-5* are thus iterative, with new ideas and framework developments being trialled and rigorously tested to assess advancement of the framework towards the goal of satisfactorily fulfilling the research objectives underpinning the research question addressed by this thesis.

To ensure an equitable and repeatable critical performance analysis of the new framework (*Step 5),* it needs to be implemented and tested under a wide range of conditions. As earlier

highlighted, a real-world MANET testbed would be ideal for providing trustworthy results. However, simulation environments offer greater flexibility as well as faster development cycles and verification iterations. They also importantly represent a more cost effective solution compared to having to construct a real MANET testbed. These were the main reasons to choose a simulation environment for development and performance analysis purposes of the new framework.

Several different network simulators are available for realistic MANET simulation purposes with OPNET, GlomoSim, OMNeT++, and *network simulator* (ns) versions 1 to 3 being popular and widely-used examples (Mallapur & Patil, 2012). As a simulation platform for testing the new framework, *ns-2* was chosen since it has been extensively used for MANET simulations and is widely accepted among the research community (Kurkowski, et al., 2005). *ns-2* also provides powerful and flexible scripting and simulation setups, common routing protocols like AODV are implemented by default, and it supports easy implementation of multiple nodes and realistic mobility models (Sarkar & McHaney, 2012). *ns-2* was installed on a PC with details of the computing platform specifications being given in Table 4.1.

Table 4.1: Detailed simulation platform specifications.

Simulation software	**PC Specifications**	
ns version 2.34	Processor	Intel ® CoreTM i3-2310M 2.10GHz
	RAM	8 Gb
	Hard Disk	167 Gb
	OS	Debian 7.0

A customised *ns-2* plugin for simulating variable packet processing times was also designed and implemented in the simulation software to rigorously evaluate the performance of the ΔTVE algorithm. This plugin was seamlessly incorporated into the simulation environment which was used throughout the performance analysis of the framework. This environment will now be formally detailed.

4.3. The Simulation Environment

This Section describes the simulation environment, including relevant input parameters and simulation output data used for evaluating the performance of the wormhole detection framework in comparison with existing solutions. Several different test cases were designed, with each individual test case consisting of a series of specific parameter settings covering for example, the type and length of the wormhole, the environment, i.e. indoors or outdoors, and the ensuing implications for node radio ranges. The complete list of relevant simulation parameters is shown in Table 4.2.

Table 4.2: Relevant simulation parameters used for each test case.

Parameter	Settings
Node wireless hardware	*IEEE 802.11n compliant*
Packet propagation speed (S)	$3 \cdot 10^8$ *m/s*
Propagation Model	*TwoRayGround* (Goldsmith, 2005)
Number of nodes	N
Network width	W
Network length	L
Wormhole length	r_{wh}
Maximum radio range	R
Number of infected (healthy) route samples	N_{IR} (N_{HR})

The simulation environment that has been developed assumes IEEE 802.11n compliant node hardware, providing a maximum radio range of 250 m when two communicating nodes are LOS (outdoors), and 70 m indoors, where the paths between nodes are assumed to be obstructed by obstacles such as walls (Barker et al., 2015). In this environment R=250 m, reflects an outdoor environment and correspondingly R = 70 m an indoor environment. For simplicity, the TwoRayGround propagation model is used throughout even though it was specifically designed for LOS. Instead, variations in node radio ranges are simulated by introducing a random instantaneous maximum radio range value R_i at each node, where

$max(R_i) = R$, so a node always has a circled coverage, but R_i can vary to reflect the impact of different obstacles around specific nodes and variabilities in antenna capability.

Every test case included either a specific N_{IR} for wormhole/time tampering detection evaluation or an N_{HR} value for *false positive* (FP) detection evaluation. For each simulation run, all nodes except the wormhole nodes, were assigned new random positions. The node hardware, S value, and the propagation model were assumed fixed throughout, while parameters N, W, L, r_{wh}, and R were varied in each test case. For wormhole detection evaluation two wormhole nodes were strategically placed in the centre, a specific distance (r_{wh}) apart, to disrupt as much traffic as possible between all network nodes. All four wormhole variants were implemented, i.e. *participation mode* (PM), *hidden mode* (HM), *in-band* (I-B), and *out-of-band* (O-B), with each being tested separately. The wormhole link delay t_{wh} for an O-B link was defined as r_{wh}/S. This mirrors the circumstances where a wormhole with a direct wireless link is established between the two malicious nodes by means of a directional antenna. For I-B links, at the beginning of each simulation run, the shortest route between two wormhole nodes was firstly requested using AODV for tunnelling routing packets. In contrast, during the FP detection experiments, no wormholes were implemented in the network area.

A visualisation output example of one simulation run is shown in Figure 4.2. with $W = L =$ 50 m, $R_{0...19} = 10$ m, $r_{wh} = 30$ m, $N = 20$, node #2 as the source, and node #3 as the destination, while nodes #0 and #1 form a PM O-B wormhole. In this example the obtained route, i.e. #2→#19→#0→#1→#16→#3, goes through the wormhole.

To simulate node movements during the route discovery procedure the *random waypoint mobility* (RWM) model, introduced by Johnson & Maltz (1996) has been adopted. In RWM, each node selects a random destination within the simulation area and then moves towards

the destination along a straight line with a randomly selected speed. While several mobility models have been proposed, including *random direction* (Royer et al., 2001), *random walk* (Camp et al., 2002), and *random Gauss-Markov* (Liang & Haas, 1999), RWM is the most popular mobility model for evaluating MANET routing protocols, mainly due to its simplicity and wide availability (Gupta et al., 2013).

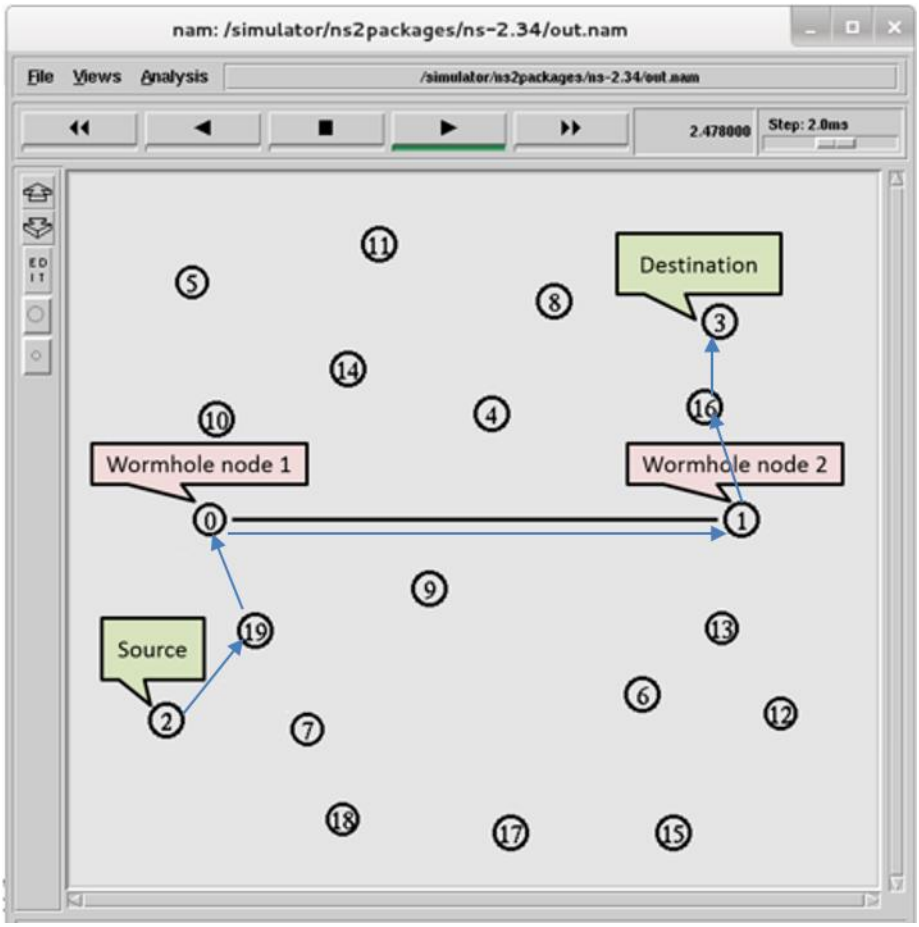

Figure 4.2: A visual output of one simulation run example.

One of the major contributions from the new wormhole detection framework involves the development of an algorithm for identifying time measurement tampering in wormhole detection with TTHCA and TTpHA. Time tampering means that malicious nodes provide fictive measurement values for the sum of the RREQ and RREP packet processing times (ΔT_i) used in the PTT calculations. The processing time of a routing packet includes the packet service time (T_S) and the *queuing delay*. These can vary because of diverse node

hardware and dissimilar traffic loads (ρ) on the nodes. One constraint on using *ns-2* is that all nodes are assumed to have identical hardware, which means that packet processing delay variabilities are dependent only upon the traffic loads ρ of each node. As there is no straightforward way of introducing specific variation levels into either T_S or ρ in the simulation environment, a special customised *ns-2* plugin for simulating different ΔT_i values was therefore designed. This plugin, as with all standard protocol implementations in *ns-2*, was programmed in C++. When using this plugin, the packet processing time measurement process implemented by TTHCA and TTpHA, which occurs at the physical layer of each node, is replaced by the new time calculation procedure illustrated in Figure 4.3. In this procedure, the normal RREQ packet processing time ($\{\Delta T_{RREQ}\}_i$) calculation, i.e., the time between receiving and forwarding a RREQ packet ($\{T_{RREQs}\}_i - \{T_{RREQr}\}_i$), is replaced by a call to subroutine *getPPTime* which returns a packet processing delay value based on the given T_S and ρ values. Full details of this customised *ns-2* plugin will be presented in Chapter 7.

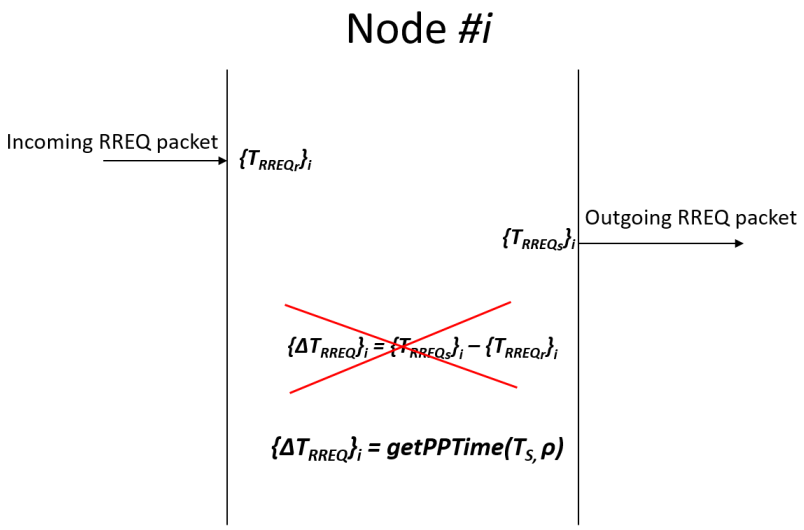

Figure 4.3: The packet processing time measurement process at a node *i* when applying the custom *ns-2* plugin, using a RREQ as an example.

The simulation output for each test case, comprises the number of correctly detected infected

routes (D_C) for wormhole/time tampering evaluation and the number of healthy routes falsely detected as infected (D_F) for FP detection evaluation. These parameters are used to calculate the performance metrics used with critical results evaluation which will now be defined.

4.4. Performance Metrics and Evaluation

To assess the wormhole, time tampering, and FP detection performance of the framework, the wormhole/time tampering *detection rate* and *FP rate* were determined separately in the simulation environment for several test MANET scenarios. These metrics have been widely used in related research papers for performance evaluation including in (Vandana & Devaraj, 2013; Dong et al., 2011; Tran et al., 2007). To generate sufficient sample data for wormhole/time tampering detection evaluation for each test case, simulation runs were repeated until N_{IR} different infected routes were collected. The wormhole/time tampering *detection rate* was then calculated as

$$Detection\ rate = \frac{D_C}{N_{IR}} \tag{4.1}$$

The *FP rate* is correspondingly given by

$$FP\ rate = \frac{D_F}{N_{HR}} \tag{4.2}$$

where N_{HR} is the number of collected healthy routes. To quantify the improvements in the wormhole/time tampering detection and *FP rate* performance of the new algorithms, a comparative performance analysis was undertaken with two established packet delay based solutions, namely DelPHI (Chiu & Lui, 2006) and M-TTM (Qazi et al., 2013). They were for evaluation purposes both implemented in the same simulation environment as the new framework. DelPHI is a natural choice as a comparator since it analyses the average packet DPH, except that DelPHI focuses on *round trip time* (RTT) rather than *packet traversal time*

(PTT) as in the new framework. Similarly M-TTM is used because it relies on PTT per hop analysis, though it makes a number of key network parameter value assumptions in its detection mechanism. These assumptions will be critically analysed and subsequently relaxed in the contribution Chapters. Finally, MHA was chosen as the comparator for TTHCA since it is an effective, existing *hop count* (HC) based solution that answers the overarching research question.

No comparative solutions were available for the time tampering detection performance evaluation since ΔTVE is the only existing proposal for detecting time tampering attacks in packet delay based wormhole detection algorithms. In considering both wormhole and time tampering detection, the ultimate outcome would be a 100% *detection rate* and 0% *FP rate* thereby accomplishing maximum security and the best QoS level. However a more pragmatic choice of ground truths were made based upon the limitations of related wormhole detection techniques discussed in the previous chapter. This involves specifying a *wormhole detection rate* $\geq$ 70% and *FP rate* $\leq$ 30% as the baseline comparators in the subsequent results analysis. The rationale for these values is the fact that with the strategic placement of a wormhole in a MANET, which has uniformly distributed nodes, approximately up to one third of all network traffic is attracted (Khabbazian et al., 2009). Therefore a minimum detection rate of 70% means in practice that the risk of obtaining a wormhole infected route decreases from $\approx$ 33% to < 10%, which is a significant improvement. A FP detection, on the other hand, means that the shortest route cannot be used between two communicating nodes and that there will be a delay in the route discovery process, since additional iterations will be needed. A 30% *FP rate* implies that the probability for two subsequent FP detections is already < 0.1 meaning in the vast majority of cases, no more than one additional route discovery process iteration is required as a result of FP detection in the new framework. Using this reasoning, a *minimum tolerable detection rate (70%)* and a *maximum tolerable FP rate (30%)* were defined as the ground truths in the ensuing results analyses.

4.5. Validation of Software Implementation and Simulation Results

To validate all software code implementations and the trustworthiness in the comparative simulation results, code correctness checking techniques and statistical significance tests for the results were used throughout the development and performance evaluation cycles of the new framework. The specific correctness check techniques used, in this thesis referred to as software code validation, will be described in the next subsection, while the rationale for the adopted statistical significance test is described in Section 4.5.2.

4.5.1. Software Code Validation

As *ns-2* was used as a platform for the simulation environment, all generic MANET related functionalities including the AODV routing protocol were already implemented, so the only new software implementations were those relating to the custom *ns-2* plugin and the constituent framework algorithms i.e., TTHCA, TTpHA, and ΔTVE extensions, together with the wormhole and time tampering attack functions. Throughout the development of these implementations both static and dynamic tests were undertaken to validate the code. A static analysis tool called *Cppcheck* (Sourceforge, 2015), was applied for detecting coding and design errors, like divide by zero, integer overflow and exception handling.

The correct behaviour of the code implementation of each contribution and comparator was manually checked by designing a number of test cases. For these dynamic tests, nodes were assigned static positions in the simulation environment and thus predicted results relating to the PTT, RTT and routing packet processing time (ΔT_i) measurements as well as wormhole/time tampering detection algorithm output could be calculated prior to each simulation run and compared to the corresponding simulation output. To rigorously validate each wormhole/time tampering detection algorithm implementation a number of targeted scenarios were generated, in which the outcome for each algorithm was known *a priori* as to whether it would fail and/or succeed. Finally, the functionality of the custom *ns-2* plugin

was validated in a similar way by manually pre-calculating a number of packet processing times based on a given set of T_S and ρ values, before comparing these with the corresponding output values generated by the *getPPTime* subroutine.

4.5.2. Statistical Significance Tests

A series of statistical significance tests was undertaken to verify that an adequate number of samples were used for the critical performance analysis in comparison with other state-of-the-art wormhole detection solutions. The output of each tested wormhole detection algorithm is either *detected* or *not detected* and these can be seen as two categorical values, i.e. the *algorithm* and its *output*. Thus, the statistical significance can be verified if there is a clear association between these two variables, in other words if the choice of algorithm has an effect on the output. In contrast, if these two variables are independent, i.e. if the choice of algorithm has no effect on the output then the statistical significance cannot be verified. For statistical significance analysis, results are typically presented in a contingency table. For this purpose such a table can be structured analogously to Table 4.3 where C_1 and C_3 are the number of correctly/falsely detected routes by the framework and the comparator respectively, while C_2 and C_4 are correspondingly, the number of undetected routes.

Table 4.3: Wormhole and FP detection simulation results plotted in a contingency table for statistical significance analysis.

Detection algorithm	**Output**	
	Detected	*Not detected*
Framework	C_1	C_2
Comparator	C_3	C_4

To analyse such 2 x 2 contingency tables for statistical significance, techniques including *Chi-square test of independence*, *Fisher's exact test*, and *the G-test* can be applied (McDonald, 2014). For this purpose, there were some restrictions relating to the choice of test technique as there are many occasions where a given cell frequency (C_1, C_2, C_3 or C_4)

may be small, for example $C_2 = 0$ in cases where the *detection rate* is 100% for the framework contribution. For this reason, neither the *G-test* nor *Chi-square* test can be applied because they require a minimum cell frequency of 5, otherwise at lower cell frequencies the results become inaccurate. In contrast, the *Fisher's exact test* is applicable regardless of cell frequency and consequently this is the rationale for applying this particular test in the results analysis. The wormhole *detection* and *FP rates* were tested separately and the hypotheses for these tests defined as:

H_0: Wormhole detection/FP rate is independent of the applied WH detection algorithm

H_1: Wormhole detection/FP rate is not independent of the applied WH detection algorithm

H_0 indicates that regardless of the applied detection algorithm, wormhole *detection rate/FP rate* will still be similar. Therefore to prove the statistical significance of the performance improvements of the two wormhole detection algorithms (TTHCA and TTpHA) compared to other state-of-the-art solutions, TTHCA and TTpHA were separately tested against each comparator algorithm. The implementation of Fisher's test is described in detail in Chapters 5 and 6.

4.6. Summary

This Chapter has provided the detailed methodology for this research. A simulation environment developed in *ns-2* has been used for critical evaluation of the performance of all thesis contributions. A detailed description of this environment has been presented together with key parameter settings, outputs, and metrics used for performance evaluation. State-of-the-art packet delay based wormhole detection algorithms, i.e. DelPHI, M-TTM, and MHA, have been implemented as comparators in the simulation environment to demonstrate the performance improvements of the new wormhole detection framework. The

statistical significance of the comparative test results have been analysed by applying *Fisher's exact test* and its implementation has been presented. The correctness of each thesis contribution and comparator code implementation in the simulation environment has been validated through both static and dynamic tests. The next chapter will introduce the first research contribution in the new wormhole attack detection framework.

5. WORMHOLE ATTACK DETECTION BASED ON TRAVERSAL TIME AND HOP COUNT ANALYSIS (TTHCA)

5.1. Introduction

As highlighted in Chapters 1 and 3, there is an absence of a unified wormhole detection solution for MANETs. This provided the main motivation for the overarching research question defined in Section 1.3 and is specifically addressed in this thesis.

Packet delay based wormhole detection techniques, such as DelPHI (Chiu & Lui, 2006), WAP (Choi et al., 2008), TTM (Tran et al., 2007), WAD-HLA (Vandana & Devaraj, 2013), NPA (Zhou et al., 2012) and the timing-based countermeasure (Khabbazian et al., 2009) were in Chapter 3 identified as potential wormhole detection solutions. These approaches offer wormhole detection mechanisms with low network overheads and require no additional hardware but most of them are based on *round trip time* (RTT) measurements and hence the assumption that variations in node packet processing times are small. In a realistic MANET, nodes can exhibit high packet processing time variations, as a consequence for example, of momentary queuing delays and/or dissimilar hardware, resulting in low wormhole *detection* and high *false positive* (*FP) rates*. The timing-based countermeasure proposed in Khabbazian et al. (2009) relaxes the aforementioned assumption by analysing *packet traversal time* (PTT) between two neighbouring nodes, where PTT is a significantly more accurate metric than RTT for estimating the distance between two nodes. However, this type of neighbour node validation is only effective for *hidden mode* (HM) wormholes since even though two *participation mode* (PM) wormhole nodes are located far apart and thus have high PTT, they can falsely inform other nodes that they have validated each other as neighbours.

To fulfil research O*bjective 1* (Section 1.3), a new wormhole attack detection algorithm based on packet *traversal time and hop count analysis* (TTHCA) is proposed and rigorously analysed in this Chapter. This algorithm is designed as an extension to AODV since this routing protocol is the most popular in the research community and is applicable in MANETs with dynamic topologies, as discussed in Chapter 2. In TTHCA, the source node first measures the RTT of the routing packets, i.e. the time from sending a RREQ until receiving the corresponding RREP. During the routing packet exchange, the processing times of the RREQ and the corresponding RREP packet (ΔT_i) are measured by each intermediate as well as by the destination node and delivered to the source node. Hence, the source node can calculate the route PTT by subtracting all ΔT_i from RTT. If PTT/HC is unrealistically high, a wormhole is suspected and a new route is requested until a healthy route is found.

The high-level and ideal aim of TTHCA is to provide 100% detection of all wormhole attack types with no false positive occurrences under any MANET scenario, while retaining negligible network overheads to provide maximum security and QoS. Though, a wormhole detection performance meeting the baseline comparator ground truths defined in Chapter 4, i.e. wormhole *detection rate* $\geq$ 70% and *FP rate* $\leq$ 30%, are already considered acceptable. For simplification, a base assumption is being made that all MANET nodes have identical hardware and are located in a *line-of-sight* (LOS) environment. In subsequent chapters, these assumptions will be both relaxed and critically analysed.

Next, the TTHCA algorithm will be described in detail and its threshold for the maximum permissible PTT/HC is critically analysed. In Chapter 5.3 a comparative simulation results analysis is provided showing superior wormhole detection performance of TTHCA compared to MHA and DelPHI. Limitations of TTHCA are also analysed as well as the impact of relaxing the identical hardware and LOS assumptions on TTHCA wormhole detection performance.

5.2. The Traversal Time and Hop Count Analysis Algorithm

TTHCA extends the AODV route discovery procedure with RTT measurements at the source node and ΔT_i measurements at the intermediate nodes as well as at the destination node. The sum of all ΔT_i (ΔT_{TOT}) is delivered to the source node for calculating PTT. The complete TTHCA extended AODV route discovery procedure is illustrated in Figure 5.1, where nodes *#0* and *#n* are the source and destination respectively, while nodes #1 through to *#i* are intermediate nodes.

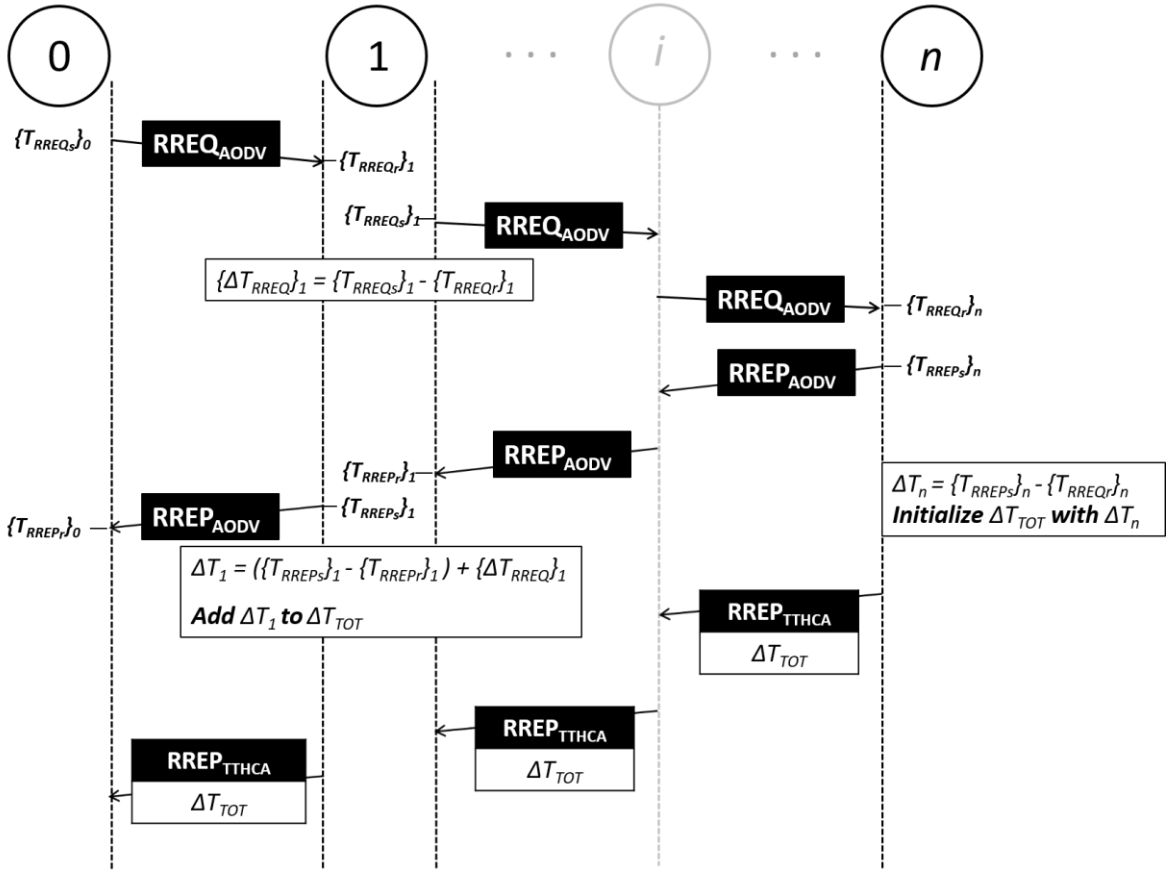

Figure 5.1: The complete TTHCA extended AODV route discovery procedure.

The source node starts the route discovery procedure by broadcasting a RREQ into the network according to the AODV routing protocol. Each node receiving a RREQ measures the processing time of the RREQ packet denoted by $\{\Delta T_{RREQ}\}_i$ (i.e. RREQ packet processing time at node #*i*) in a similar way to that proposed in Khabbazian et al. (2009), i.e. the time from receiving the first bit of the RREQ ($\{T_{RREQr}\}_i$) until sending the first bit of the forwarded

RREQ ($\{T_{RREQs}\}_i$). $\{\Delta T_{RREQ}\}_i$ is temporarily stored in local memory. When the RREQ reaches the destination node, a RREP packet is created and sent back to the source node as a unicast packet through the shortest route as in normal AODV. Correspondingly to the RREQ broadcast procedure, each intermediate node creates the timestamp $\{T_{RREPr}\}_i$ when receiving the first bit of RREP and $\{T_{RREPs}\}_i$ when sending the first bit of the forwarded RREP to the next hop. After sending the RREP, the destination node calculates $\Delta T_i = \{T_{RREPs}\}_i - T_{RREQr}\}_i$ and the intermediate nodes $\Delta T_i = \{\Delta T_{RREQ}\}_i + (\{T_{RREPs}\}_i - T_{RREPr}\}_i)$

To deliver ΔT_{TOT} to the source node, a new RREP packet ($RREP_{TTHCA}$), including a ΔT_{TOT} parameter, is generated at the destination with its ΔT_i value and sent as a unicast packet to the source after sending the original AODV RREP ($RREP_{AODV}$). Each intermediate node receiving $\text{RREP}_{\text{TTHCA}}$ adds its own ΔT_i value to the ΔT_{TOT} parameter. To achieve high resolution time stamps, the ΔT_i measurements must be performed at the physical layer while routing packets are processed at the network layer. For this reason, the ΔT_i measurement information cannot be added to $\text{RREP}_{\text{AODV}}$.

The source node records time stamps $\{T_{RREQs}\}_i$ and $\{T_{RREPr}\}_i$ when sending the RREQ and receiving the corresponding $\text{RREP}_{\text{AODV}}$ respectively and calculates the route *RTT* as follows

$$RTT = \{T_{RREPr}\}_i - \{T_{RREQs}\}_i \tag{5.1}$$

When $\text{RREP}_{\text{TTHCA}}$ is received it then calculates the route PTT as

$$PTT = \frac{RTT - \Delta T_{TOT}}{2} \tag{5.2}$$

A flowchart showing the constituent processes involved in TTHCA at the source node is shown in the Figure 5.2.

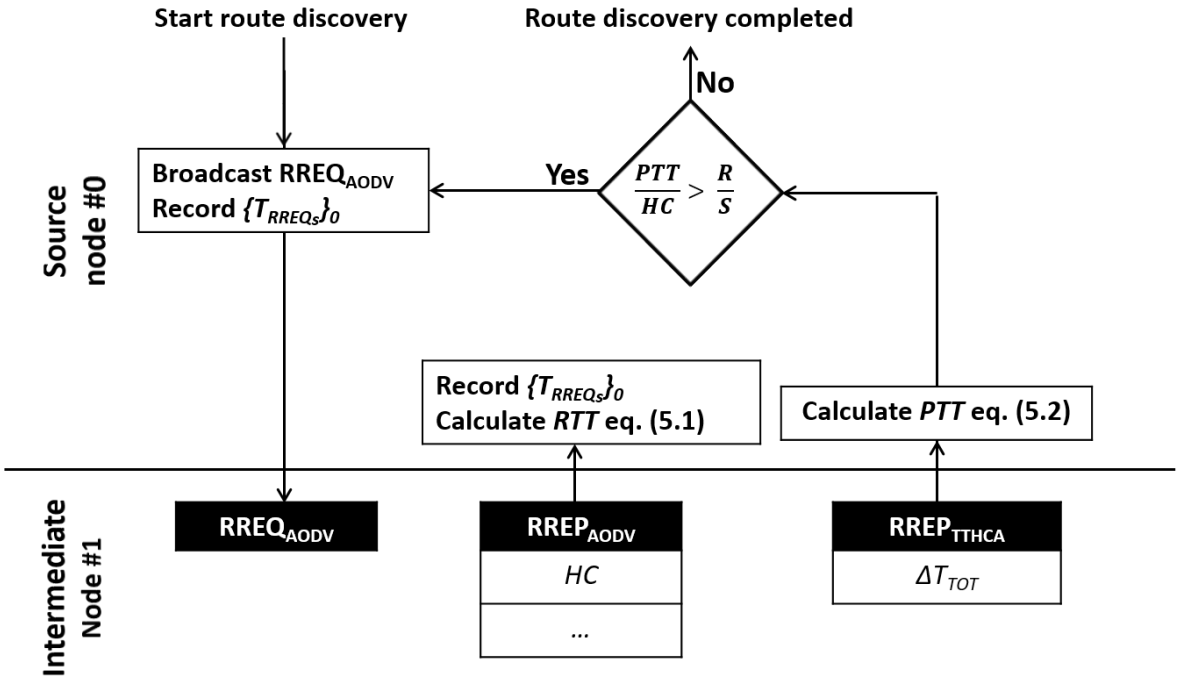

Figure 5.2: A flowchart of the TTHCA wormhole detection algorithm.

If all MANET nodes have identical hardware and are located in a LOS environment, then the maximum distance a routing packet can travel is the maximum radio range *R.* Based on this, a wormhole is suspected by TTHCA if:

$$\frac{PTT}{HC} > \frac{R}{S} \tag{5.3}$$

If the threshold in eq. (5.3) is true, then a wormhole is suspected and a new RREQ with a new sequence number is broadcasted to find a new route between the source and destination nodes. According to the AODV routing protocol, an intermediate node having a fresh route to the destination will reply with a RREP while other nodes will forward the new RREQ towards the destination. Thus, if the source node does not accept a RREP packet received from the same intermediate node as during the previous route discovery procedures, the newly requested route will be unique. This iterative route discovery process is repeated until a safe route is found. The performance of TTHCA and the fixed threshold eq. (5.3) will be critically analysed in the next Section and experimentally tested in Section 5.3.

5.2.1. *Critical Analysis of the Static Threshold*

To detect a wormhole using the threshold in eq. (5.3), the total deviation of the PTT of each legitimate hop ($PTT_{i,i+1}$ which is equivalent to $r_{i,i+1}/S$, where $r_{i,i+1}$ is the actual distance between two successive nodes) from R/S must be small relative to the wormhole link delay (t_{wh}) which is defined as:

$$t_{wh} = \frac{r_{wh}}{S} + \frac{\Delta T_{wh}}{2} \tag{5.4}$$

where r_{wh} is the length and ΔT_{wh} is the total packet processing time of the wormhole link, i.e. ΔT_{wh} is the sum of all ΔT_i at the legitimate nodes through which the malicious nodes tunnel routing packets to each other (in case of I-B wormhole) and the ΔT_i values at the wormhole nodes (in the case of a HM wormhole). In the example MANET shown in Figure 5.3, r_{wh} is the distance between wormhole nodes #3 and #6. If an HM I-B wormhole is launched then $\Delta T_{wh} = \Delta T_2 + \Delta T_6 + \Delta T_7 + \Delta T_3$ while for a PM I-B wormhole $\Delta T_{wh} = \Delta T_6 + \Delta T_7$. The difference in the two ΔT_{wh} values is because HM wormhole nodes do not process routing packets and thus they do not add their ΔT_i values to $\Delta T_{TOT.}$ Conversely, an HM O-B wormhole means that $\Delta T_{wh} = \Delta T_2 + \Delta T_3$, while $\Delta T_{wh} = 0$ for a PM O-B wormhole since the malicious nodes are able to directly tunnel routing packets to each other over a dedicated network link.

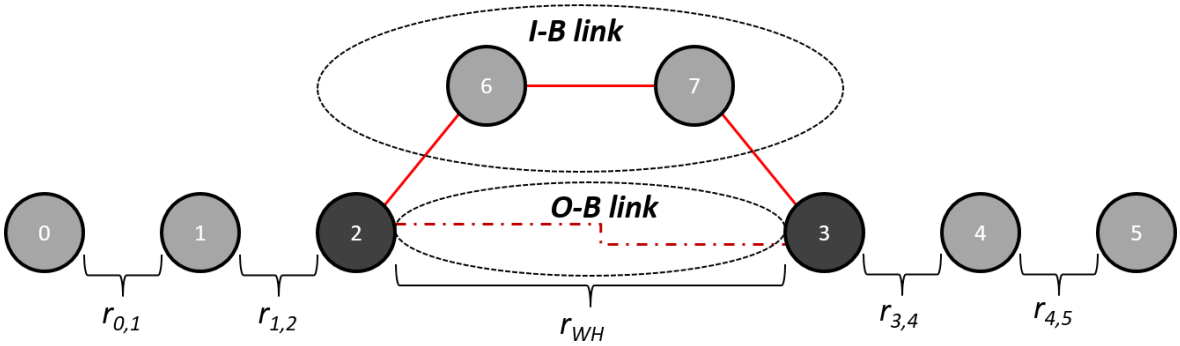

Figure 5.3: A visualization of a MANET where nodes #2 and #3 are malicious launching either an I-B or O-B wormhole, with nodes #0 and #5 being the source and destination nodes respectively.

The PTT of a wormhole infected route, as calculated by the source node, is the sum of all legitimate $PTT_{i,i+1}$ and t_{wh}:

$$\sum_{i=1}^{HC-1} \left(\frac{r_{i,i+1}}{S}\right) + t_{wh} \tag{5.5}$$

where *HC* is the route length in terms of hops as calculated by the routing protocol. So in the Figure 5.3 example, *HC* = 3 if a HM wormhole is launched (as the fictive route is #0→#1→#4→#5) and *HC* = 5 (#0→#1→#2→#3→#4→#5) for a PM wormhole.

The ideal scenario arises when $r_{i,i+1} = R$ because then the PTT of a healthy route is $HC \cdot \frac{R}{S}$ which equals the maximum permissible route PTT inferred by eq. (5.3). To be effective, r_{wh} must be > *R* so any wormhole link will lead to a condition where PTT > $HC \cdot \frac{R}{S}$ and thus be detected. However, in a realistic MANET environment where nodes are randomly distributed, $r_{i,i+1}$ is typically < *R* and therefore must lie within the bounds specified by *Lemma 5.1*.

Lemma 5.1: Assuming the maximum radio range *R* is identical for every node, then $r_{i,i+1}$ is bounded by:

$$r_{i,i+1} \leq R \tag{5.6}$$

$$(r_{i,i+1} + r_{i+1,i+2}) > R \tag{5.7}$$

Proof: Eq. (5.6) cannot be false since otherwise intermediate nodes #*i* and #*i+1* will be out of radio range coverage. Correspondingly, eq. (5.7) must be true since otherwise the 2-hop neighbour of intermediate node #*i* (#*i*+2) will still be within radio range and thus become only a 1-hop neighbour. ■

The value of the threshold in eq. (5.3) which must be upheld is formally defined in *Lemma 5.2.*

Lemma 5.2: Assuming identical *S* through both the air and on the wormhole link, then eq. (5.3) is upheld if:

$$\sum_{i=1}^{HC-1} \left(\frac{R - r_{i,i+1}}{S}\right) < t_{wh} - \frac{R}{S} \tag{5.8}$$

Proof: Eq. (5.3) implies a wormhole will be detected whenever route PTT > $HC \cdot \frac{R}{S}$, so if eq. (5.8) is false, then from eq. (5.2) the calculated PTT ≤ $HC \cdot \frac{R}{S}$, which means the wormhole will not be detected. ■

An I-B or a HM wormhole incurs a high ΔT_{wh} since routing packets are tunneled through legitimate nodes in the I-B case and HM wormhole nodes do not modify the routing packets. Routing packet processing times >> PTT and thus I-B and HM wormholes are straightforward to detect by applying the static threshold eq. (5.3) as will be shown in Section 5.3.1.

PM O-B wormholes are the most challenging for TTHCA to detect since $\Delta T_{wh} = 0$ and therefore t_{wh} is significantly smaller than for an I-B and a HM wormhole. As an illustration assume R = 100 m and that a 3-hop PM O-B wormhole exists within the MANET. This implies $r_{wh} = 3R$ so if all $r_{i,i+1}$ are closer to the lower bound eq. (5.6), e.g. 51 m, a wormhole infected route will not be detected if the route HC > 4 because then eq. (5.8) will not hold. On the other hand, if all $r_{i,i+1}$ are close to the upper bound eq. (5.7), e.g. 99 m, then a wormhole infected route would be detected for route HC up to 200. So, since $\Delta T_{wh} = 0$ the TTHCA wormhole detection performance on a PM O-B wormhole is highly dependent on the sum of all $R - r_{i,i+1}$ in relation to the length of the wormhole link, which can be derived

from eq. (5.8). This is also clearly reflected in the simulation results showing TTHCA wormhole detection performance on PM O-B wormholes with various lengths in the next Section.

5.3. Simulation and Results Analysis

The performance of TTHCA was rigorously evaluated by analysing the wormhole *detection rate* eq. *(4.1)* and the *FP rate* eq. *(4.2)* in comparison with DelPHI and MHA in the *ns-2* simulation environment described in Chapter 4. DelPHI operates in a similar manner as TTHCA in terms of route delay per HC analysis, with the significant difference being that TTHCA uses PTT rather than RTT. In this Section it will be shown how this strategy significantly improves wormhole detection performance. Correspondingly, the reason for using MHA as a comparator is to show that HC analysis as such is not adequate for robustly detecting wormholes. In the simulations it is assumed that all timestamps can be recorded with 1 ns accuracy, which is currently only possible with either specialist hardware (Microsemi, 2013) or by using a special receiver architecture on existing hardware (Exel et al., 2010). It is also assumed there is no time tampering of the ΔT_{TOT} value. These assumptions will be subsequently relaxed in Chapters 6 and 7, where timestamp accuracy and time tampering issues will be more rigorously analysed.

The specific simulation environment parameters used for these experiments are defined in Table 5.1. The rationale behind choosing large values for both network length (L) and maximum radio range (R) was to reflect an outdoor LOS environment analogously to Jen et al. (2009), while the corresponding indoor environment scenario is analysed in Chapter 6. To reflect different network environment topography i.e., square and rectangular with varying widths, W was assigned a random value during each simulation run, while the overall network area was kept constant.

Table 5.1: Specific simulation parameters used for testing TTHCA, MHA and DelPHI to reflect and outdoor LOS environment.

Parameter	Settings
N	300
W	Random value: 1500 m – 4000 m
L	$\frac{4\ 000\ 000\ \text{m}^2}{W}$
R	250 m
N_{IR} and N_{HR}	100

For DelPHI, the time threshold T = 3 ms was chosen in accordance with Chiu & Lui (2006) as this offers a pragmatic balance between *detection* and *FP rates*, while for MHA, $RREP_{lim}$ = 2 was used since when there is only one wormhole in the network, two comparable route samples are sufficient to detect the wormhole infected route. In the ensuing experimental testing, all four wormhole variants i.e. HM, PM, I-B and O-B were considered.

5.3.1. Detection Performance

In the first set of experiments, the detection performance for HM I-B/O-B and PM I-B wormholes was tested for various wormhole lengths, with the results being displayed in Figures 5.4 - 5.6. For all simulated wormhole types, the length indicates the physical distance between the two wormhole nodes and is specified in hops where *1-hop = R*, so for a 3-hop wormhole, $r_{wh} = 3R$.

TTHCA *detection rates* are consistently superior compared to DelPHI and MHA as TTHCA detected all wormholes and generated no false positives, while the respective wormhole *detection rates* for DelPHI and MHA were 30% to 60 % and 30% to 70%. When the MANET is infected by a HM wormhole, malicious nodes do not modify the routing packets, they just tunnel them to each other so the malicious nodes do not add their ΔT_i values to the ΔT_{TOT} parameter of the RREP packet. Hence, the delay of the wormhole link (t_{wh}) is significantly

higher than any hop PTT $(PTT_{i,i+1})$ and therefore the condition eq. (5.8) in *Lemma 5.2* is always met.

HM I-B wormholes incur even higher t_{wh} than HM O-B wormholes since malicious nodes tunnel routing packets to each other through other legitimate nodes. So, t_{wh} will in the HM I-B wormhole case include both packet processing times of the wormhole nodes as well as of the legitimate nodes through which the routing packets were tunneled and so again *Lemma 5.2* is always fulfilled.

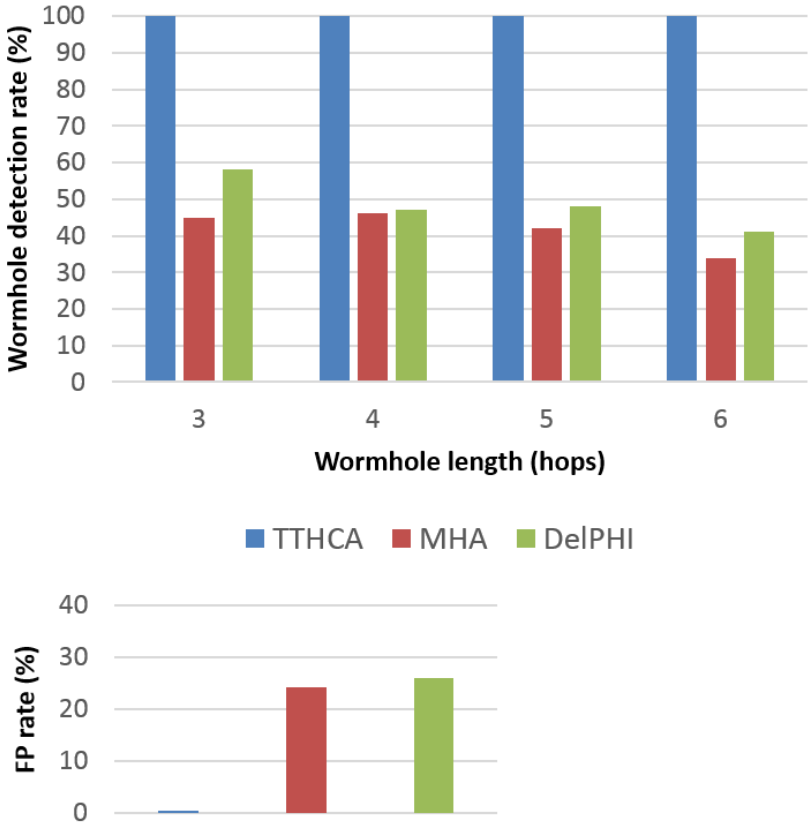

Figure 5.4: Comparative HM O-B wormhole and FP detection performance.

Even though HM O-B/I-B and PM I-B wormhole links are significantly slower than PM O-B wormhole links, the detection performance of DelPHI in contrast is generally poor. The reason for this is the variation in packet processing times and the occurrence of queuing delays which typically are much greater than packet service times. If for example, one or

more nodes on a fresh route cause queueing delays, the RTT/HC of that route may potentially be higher than the RTT/HC of a wormhole infected route where no queuing delays are experienced. For the same reason, the *FP rate* for DelPHI is correspondingly higher for all wormhole types

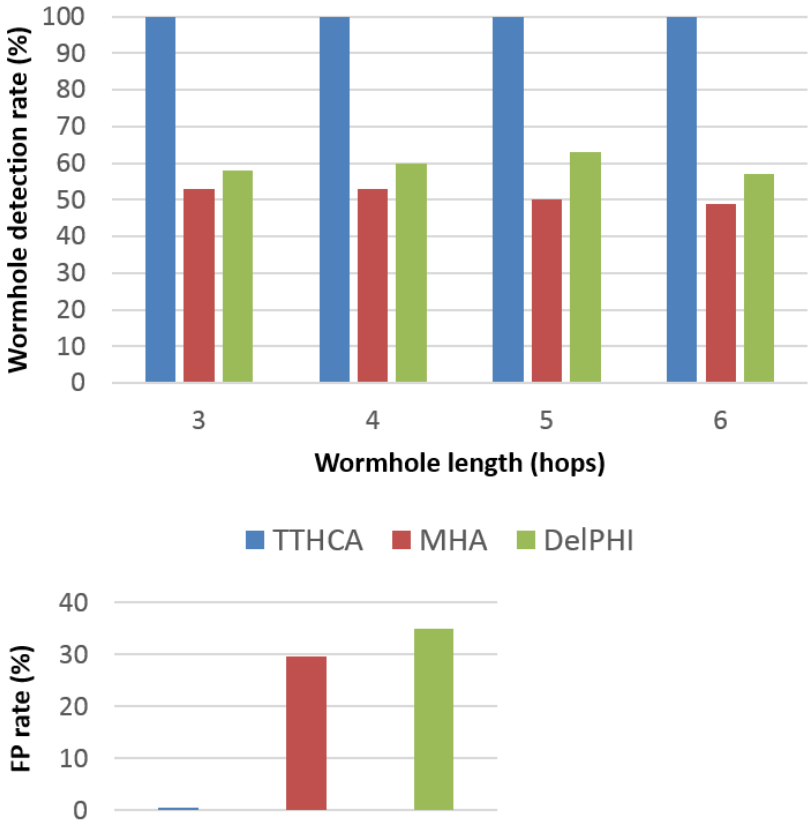

Figure 5.5: Comparative HM I-B wormhole and FP detection performance.

In the next set of experiments, the comparative wormhole attack detection performance for a PM O-B wormhole is analysed and the results plotted in Figure 5.7. As discussed in Section 5.2.1, the PM O-B wormhole is the most challenging to detect for TTHCA since $\Delta T_{wh} = 0$ and therefore the only delay caused by the wormhole link is the PTT between the malicious nodes. This is reflected in the detection performance as 100% wormhole detection is only achieved when the wormhole is > 6 hops due to the fact that then the wormhole link is long enough for the condition defined in eq. (5.8) to always uphold. When decreasing the length of the wormhole link, the *detection rate* progressively starts to drop. Though, a wormhole ≥

4 hops is still detected with a likelihood of > 90% which is significantly higher than the baseline comparator ground truth (70%) defined in Chapter 4. However, TTHCA cannot robustly detect PM O-B wormholes < 4 hops due to the fact that then the sum of all $R - r_{i,i+1}$ is often large in relation to the wormhole length and hence the eq. (5.8) condition will not hold.

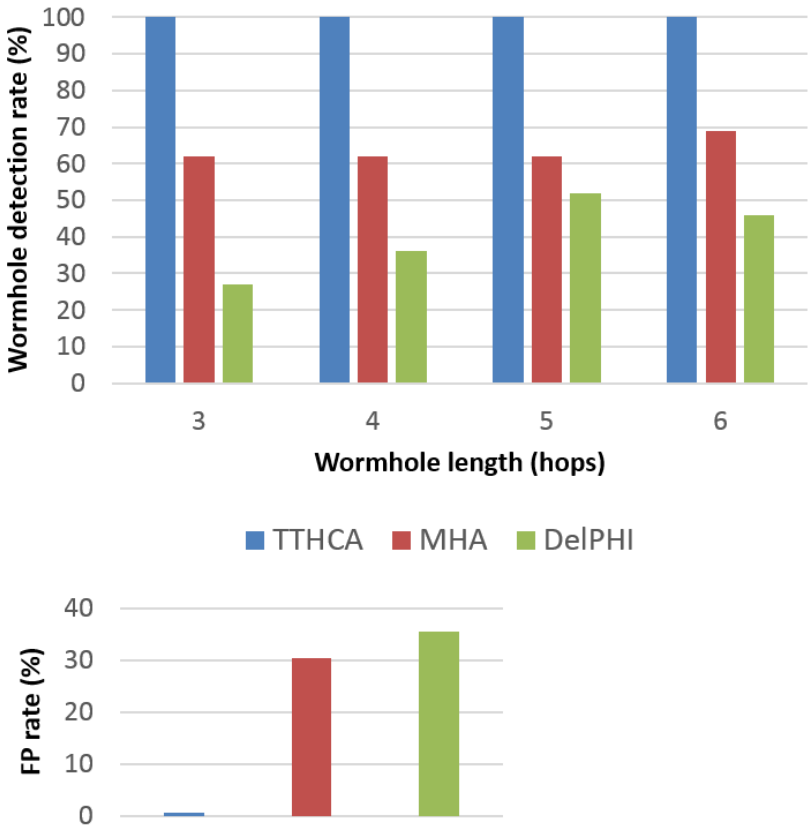

Figure 5.6: Comparative PM I-B wormhole and FP detection performance.

DelPHI was unable in practice, to detect any PM O-B wormholes since the *FP rates* were always higher than the wormhole *detection rate*. The difference between the wormhole link delay (t_{wh}) and any hop packet traversal time ($PTT_{i,i+1}$), for a PM O-B wormhole is negligibly small compared to variations in packet processing times and so it is not possible for DelPHI to distinguish between an infected and a healthy route.

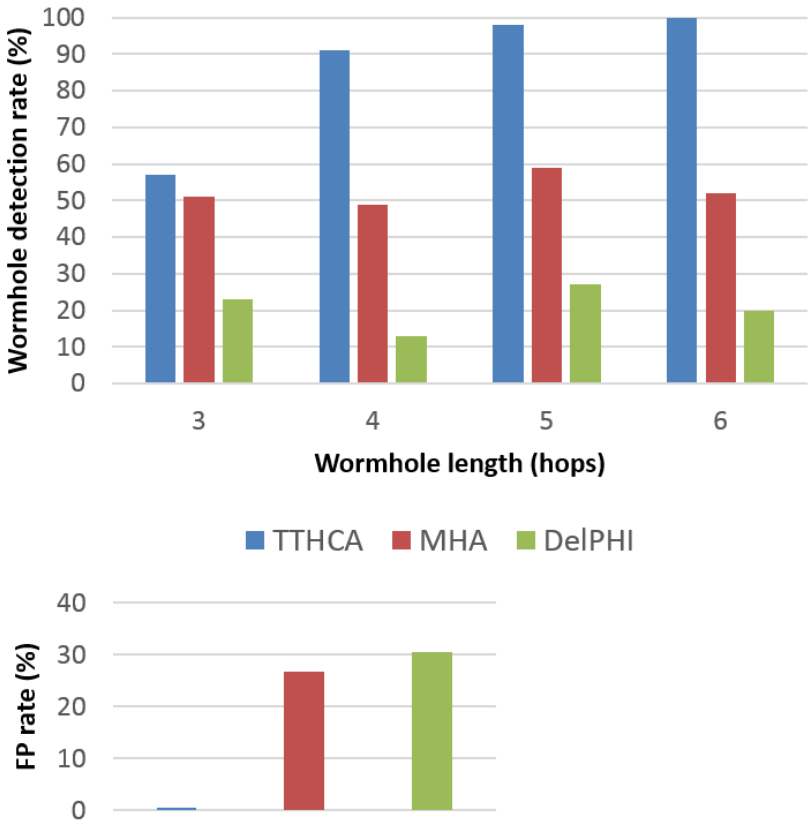

Figure 5.7: Comparative PM O-B wormhole and FP detection performance.

For MHA, the value of t_{wh} is immaterial since it only analyses route HC in its wormhole detection mechanism. It was though revealed from the test results that MHA is ineffective on all tested wormhole types as the detection rate is poor (between 35% and 70%) in all cases. Under these circumstances where all nodes were randomly distributed in the simulation test area there were many instances where the wormhole link did not have the shortest HC, which decreases the detection rate while commensurately increasing the likelihood of false positives. There are also many cases where the HC of the shortest route is significantly smaller than the HC of the second shortest route, which also generates FP detections. The detection performance was slightly better for PM wormholes (between 50 and 70%) compared to HM wormholes (between 35 and 50%). The reason is that there is a risk for all routes to traverse the HM wormhole during the MHA extended AODV route discovery since HM wormhole nodes cannot be included in the *graylist* as discussed in Chapter 3.

5.3.2. Statistical Significance Analysis

To evaluate the statistical significance of the results presented in the previous Section, which show clear wormhole and FP detection performance improvements for TTHCA compared to DelPHI and MHA, *Fisher's exact test* was applied as explained in Chapter 4. In short, the rationale behind this test was to determine whether the choice of wormhole detection mechanism is related to the wormhole *detection* and *FP rate*. The hypotheses were defined as follows:

H_0: TTHCA performance = MHA/DelPHI performance

H_1: TTHCA performance ≠ MHA/DelPHI performance

The test results for all wormhole types, i.e. HM, PM, O-B, and I-B, are presented Table 5.2. They show that the wormhole *detection* and *FP rate* differences observed between TTHCA and DelPHI are statistically significant for all wormhole variants as H_0 was false by a clear margin. Similarly, the differences between TTHCA and MHA in *FP rates* are also statistically significant for all test cases. When wormhole detection for TTHCA in comparison to MHA is considered, H_o was false in all cases except for PM O-B wormholes shorter than 4 hops, where only a marginal difference was observed with corresponding detection rates of 57% for TTHCA compared to 51% for MHA.

To summarise, these statistical significance tests indicate that an adequate amount of samples have been generated in the simulations for producing comparative wormhole detection and FP performance results for TTHCA vs. MHA as well as TTHCA vs. DelPHI showing clear improvements of TTHCA. The only exception is the 3-hop PM O-B wormhole case where the conclusion can be drawn MHA and TTHCA wormhole detection performance is equivalent.

Table 5.2: Fisher's exact test results for wormhole detection and FP performance where *p* is the probability for that H_0 is true.

<table>
<tr><th colspan="2">Wormhole variants</th><th rowspan="2">Result type</th><th rowspan="2">TTHCA vs. MHA</th><th rowspan="2">TTHCA vs. DelPHI</th></tr>
<tr><th>Type</th><th>Length (hops)</th></tr>
<tr><td rowspan="2">HM I-B
HM O-B
PM I-B</td><td rowspan="2">3–6</td><td>Wormhole</td><td colspan="2" rowspan="2">H₀ = false
(p < 0.0001)</td></tr>
<tr><td>FP</td></tr>
<tr><td rowspan="4">PM O-B</td><td rowspan="2">3</td><td>Wormhole</td><td>H₀ = true
(p = 0.4782)</td><td rowspan="2">H₀ = false
(p < 0.0001)</td></tr>
<tr><td>FP</td><td>H₀ = False
(p < 0.0001)</td></tr>
<tr><td rowspan="2">4–6</td><td>Wormhole</td><td colspan="2" rowspan="2">H₀ = false
(p < 0.0001)</td></tr>
<tr><td>FP</td></tr>
</table>

5.3.3. Network Overheads

The destination and intermediate nodes only perform addition and subtraction operations for calculating routing packet processing delays (ΔT_i), while the source node performs a subtraction to calculate round trip time, a subtraction and division for calculating packet traversal time in eq. (5.2) and two division operations for the wormhole threshold check in eq. (5.3). All these calculations together on the destination node and the intermediate nodes have linear complexity *O(HC).*

Due to the requirement for an additional routing packet, $\text{RREP}_{\text{TTHCA}}$, when applying TTHCA in AODV, there will be an increased delay incurred in the route discovery process which can be expressed as:

$$\sum_{i=1}^{HC}(\{\Delta T_{RREP\_TTHCA}\}_i + \frac{r_{i,i+1,}}{S})\ seconds \tag{5.9}$$

where $\{\Delta T_{RREP\_TTHCA}\}_i$ is the $\text{RREP}_{\text{TTHCA}}$ packet processing time at intermediate node *i*. This delay is small however, compared to MHA where the route discovery procedure must always be performed at least twice to be able to perform the HC analysis algorithm. In contrast,

TTHCA only requires a single RREQ broadcast operation if the first obtained route is healthy. DelPHI also requires only one RREP per route discovery but incurs a higher load on the network compared to both MHA and TTHCA because it uses a modified version of the AODV protocol to identify all possible routes between the source and destination node.

5.3.4. Results Discussion

The presented results confirm that TTHCA pragmatically fulfils the research *Objective 1* to accurately and consistently detect HM/PM O-B and PM I-B wormholes with no false positive detection occurring. Any route infected by either a HM/PM O-B or PM I-B wormhole is straightforward to distinguish from a healthy route since it leads to a significantly higher PTT/HC due to the high ΔT_{wh} value which leads eq. (5.8) to be upheld. The high *detection rate* is not always met however, when the MANET is infected by a PM O-B wormhole and the wormhole link is short, i.e. less than 6 hops in the test simulation environment. This is true because $\Delta T_{wh} = 0$ for such a wormhole and therefore a long route with a short wormhole means that *Lemma 5.2* is not fulfilled and the wormhole is undetected. Though the *detection rate* is higher than the defined baseline comparator ground truth (70%) when the wormhole length $\geq$ 4 hops.

From a computational and network complexity perspective, TTHCA offers a low overhead solution as all the operations have linear complexity *O(HC).* However, the new routing packet $\text{RREP}_{\text{TTHCA}}$ introduces an extra delay in the route discovery procedure and some additional packet processing at both the intermediate and destination nodes is incurred because TTHCA requires two reply packets instead of one in the AODV protocol.

A summary of the high level aims to fulfil *Objective 1* and how the proposed TTHCA algorithm fulfils these goals when nodes have identical hardware and are in LOS is presented in Table 5.3.

Table 5.3: A summary of desired goal settings for TTHCA and how they were fulfilled.

Desired goal settings	TTHCA	
	Objective achieved?	Summary
100% wormhole detection	*Partially*	Detection rate is 100% for HM/PM O-B and PM I-B wormholes but < 100% for short PM O-B wormholes.
Network topology independent	*Partially*	A short PM O-B wormhole in relation to the route HC is not detected.
No FP detection	*Yes*	Assuming accurate RTT and ΔT_i measurements eq. (5.3) can never be true for a healthy route.
Low computational overheads	*Yes*	All computational operations have order of complexity *O(HC)*
Negligible bandwidth load	*Partially*	New routing packet $RREP_{TTHCA}$ causes a minor delay on the routing discovery procedure and bandwidth overheads on intermediate nodes.

Using the fixed threshold in eq. (5.3) has proven to work well provided all nodes have same *R* and are located in a LOS environment. However, the wormhole detection rate degrades once the aforementioned assumptions are relaxed, such as for instance, high variability in radio coverage, which can be experienced due to different MANET node hardware and/or variability in network surroundings.

To illustrate the effect of relaxing the LOS environment assumption on TTHCA wormhole detection performance, consider the 5 HC route example in Figure 5.8, where A and D are the source and destination nodes respectively, M_1 and M_2 are malicious PM O-B wormhole nodes, and B as well as C are legitimate intermediate nodes.

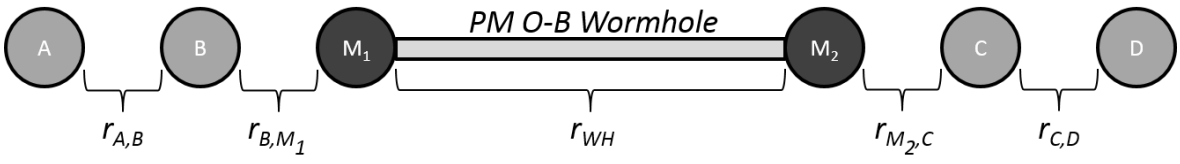

Figure 5.8: An example of a route infected by a PM O-B wormhole.

Assuming identical node hardware with R = 100 m, and all $r_{i,i+1}$ values being close to the lower bound eq. (5.6) in *Lemma 5.1*, such as 51 m. If the wormhole link is *3R* (3 hops) then

the corresponding PTT for that route will be $\frac{\sum_{i=1}^{HC-1} r_{i,i+1}+r_{wh}}{S}$ = 1680 ns and the wormhole will in a LOS environment be detected, but only within the very narrow window ($\frac{PTT}{HC} = 336ns > \frac{R}{S} = 333ns$) from eq. (5.3). If however, there are physical obstacles between two or more nodes on the A to D path, the lower bound for $r_{i,i+1}$ between these nodes will inevitably become lower than eq. (5.6) and as a result there is a higher likelihood the wormhole will not be detected. For example, if $r_{A,B}$ = 44 m due to an obstacle between A and B, while all remaining $r_{i,i+1}$ = 51 m, PTT/HC will then = 332 ns which is less than *R/S* so the wormhole will not be detected using the static threshold in eq. (5.3).

The impact of relaxing the assumptions on network environment and node hardware is rigorously analysed in Chapter 6 where a new extended version of TTHCA, called TTpHA is presented which integrates a dynamic threshold mechanism which is able to adapt to the prevailing network conditions and thus provides improved wormhole detection performance in challenging environments where there are high radio range variations.

5.4. Summary

This Chapter has presented a new wormhole detection algorithm, TTHCA, that is based on PTT/HC analysis. Similarly to the RTT based approach DelPHI, TTHCA analyses the delay of a route in relation to its HC for identifying a wormhole infected route, however unlike DelPHI and other RTT-based solutions, it reduces all node packet processing delays from the RTT measurement to get the PTT. PTT more accurately reflects the distance of a route compared to RTT and is therefore significantly more robust for detecting wormholes.

Simulation results showed that TTHCA works well when assuming LOS environments and identical hardware on all nodes and therefore TTHCA fulfils *Objective 1* to a satisfactory standard. TTHCA wormhole detection and false positive performance was also significantly

better compared to DelPHI and MHA. However, if the route is infected by a short PM O-B wormhole in relation to the route HC there is a risk that TTHCA wormhole detection will fail. High fluctuations in radio ranges further increase the risk that TTHCA will not detect PM O-B wormholes. TTHCA uses a fixed threshold for PTT/HC validation which has two main limitations, firstly it does not adapt to prevailing network conditions meaning that the wormhole detection performance in an indoor environment is poor since such an environment requires a lower threshold than a LOS environment. Secondly, in a heterogeneous network where network nodes are using dissimilar wireless communication technologies the threshold for the maximum permissible PTT/HC cannot be based on *R* since it may be highly variable even in a LOS environment.

To address the identified limitations of TTHCA in node radio range variability and fulfill research *Objective 2,* a new extended version of TTHCA, called TTpHA is proposed in the next Chapter.

6. WORMHOLE ATTACK DETECTION USING PACKET TRAVERSAL TIME PER HOP ANALYSIS WITH DYNAMIC THRESHOLD

6.1. Introduction

To address the limitations of TTHCA identified in Chapter 5 in regard to using a static threshold in the *packet traversal time* (PTT) per *hop count* (HC) analysis, this Chapter introduces a new flexible wormhole attack detection technique called *traversal time per hop analysis* (TTpHA), which employs a dynamic threshold for the maximum permissible PTT for each hop. This feature enables TTpHA to automatically adapt to prevailing network conditions and handle variable node radio ranges. Analysing the delay for each hop is a more accurate approach to wormhole detection than average hop delay analysis. This observation was firstly identified in *round trip time* (RTT)-based approaches like WAP (Choi et al., 2008), TTM (Tran, Hung et al. 2007), and then more recently in a modified variant of TTM (M-TTM) (Qazi et al., 2013).

A key factor in any packet delay based wormhole detection technique is the accuracy of the timestamps recorded for incoming and outgoing routing packets. This Chapter includes a critical analysis of the requirements on the *timestamp resolution* (TR) for TTpHA and provides comparative evaluation of wormhole detection performance between TTpHA and M-TTM for different TR values and network conditions. The impact of node mobility during the route discovery procedure on wormhole attack detection performance is also evaluated for TTpHA and M-TTM. Without loss of generality, the focus in this Chapter will be upon *participation mode* (PM) *out-of-band* (O-B) wormholes as these are the most challenging to detect. The same broad design objectives are set for TTpHA as for TTHCA, though the assumptions of identical and high timestamp resolution hardware nodes located in a *line-of-sight* (LOS) environment are relaxed.

6.2. The Packet Traversal Time per Hop Analysis Algorithm

TTpHA is a major extension to the original TTHCA algorithm presented in Chapter 5, embracing two significant improvements:

i) TTpHA measures and analyses PTT for each successive hop ($PTT_{i,i+1}$) rather than PTT/HC to provide more accurate wormhole attack detection.

ii) TTpHA uses a dynamic threshold for the maximum permissible $PTT_{i,i+1}$ to automatically adapt to variable radio ranges and network environments.

In this Section, the extended TTpHA route discovery procedure employed to determine the $PTT_{i,i+1}$ calculations is firstly discussed, before a critical analysis of the new dynamic threshold mechanism is presented.

6.2.1. TTpHA Extended AODV Route Discovery Procedure

TTpHA operates just as the TTHCA algorithm in broadcasting $RREQ_{AODV}$ packets, but the procedure at the intermediate nodes is extended in receiving and sending RREP messages. Each intermediate node calculates not only routing packet processing times (ΔT_i), as in TTHCA, but also the PTT between itself and the destination node (PTT_i), which is then inserted as an element of a new dedicated PTT_i vector parameter in the $RREP_{TTpHA}$ packet. PTT_i is determined at each intermediate node upon receipt of a $RREP_{AODV}$ packet according to eq. (5.2). To clarify the difference between the PTT_i and $PTT_{i,i+1}$ notation, consider the MANET scenario illustrated in Figure 5.3. In this scenario, $PTT_{1,2}$ refers to the measured traversal time of a routing packet that is sent between nodes #1 and #2, while PTT_1 refers to the packet traversal time between node #1 and the destination node.

The complete TTpHA extended route discovery procedure is illustrated in Figure 6.1, where as in Figure 5.1, node #0 is the source, nodes #1 to #*i* are intermediate nodes and #*n* is the destination node.

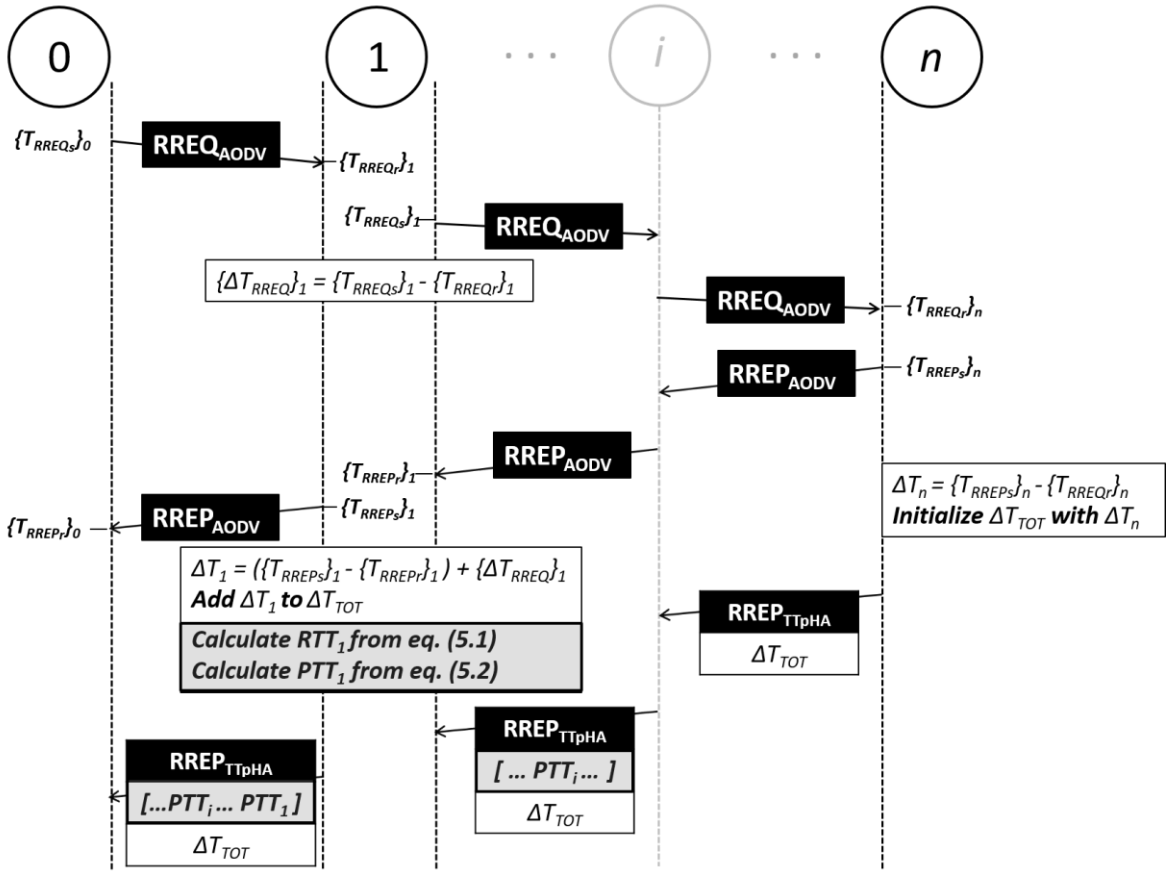

Figure 6.1: The TTpHA extended AODV route discovery procedure, with the new elements shaded in grey (all other blocks are as in TTHCA (Karlsson et al., 2011)).

In addition to the route PTT, the source node also calculates each $PTT_{i,i+1}$ from

$$PTT_{i,i+1} = PTT_i \tag{6.1}$$

where it is assumed node #$i+1$ is the destination, otherwise it sets

$$PTT_{i,i+1} = PTT_i - PTT_{i-1} \tag{6.2}$$

Each hop packet traversal time value ($PTT_{i,i+1}$) is then inserted as an element to a vector V whose elements are ranked in ascending order. V is used to determine a dynamic threshold (Θ) for the maximum permissible $PTT_{i,i+1}$ of the route. If nodes #i and #$i+1$ form a PM wormhole, then $PTT_{i,i+1}$ at node #i will be larger than any healthy $PTT_{i,\,i+1}$ so the wormhole link is detected if $V_{HC} > \Theta$. The situation where several wormholes exist in a MANET must also be considered for TTpHA, so all elements in V must be separately evaluated. The

complete TTpHA algorithm at the source node is shown in Figure 6.2, while the methodology used to determine the new TTpHA dynamic threshold Θ is critically analysed in next Section.

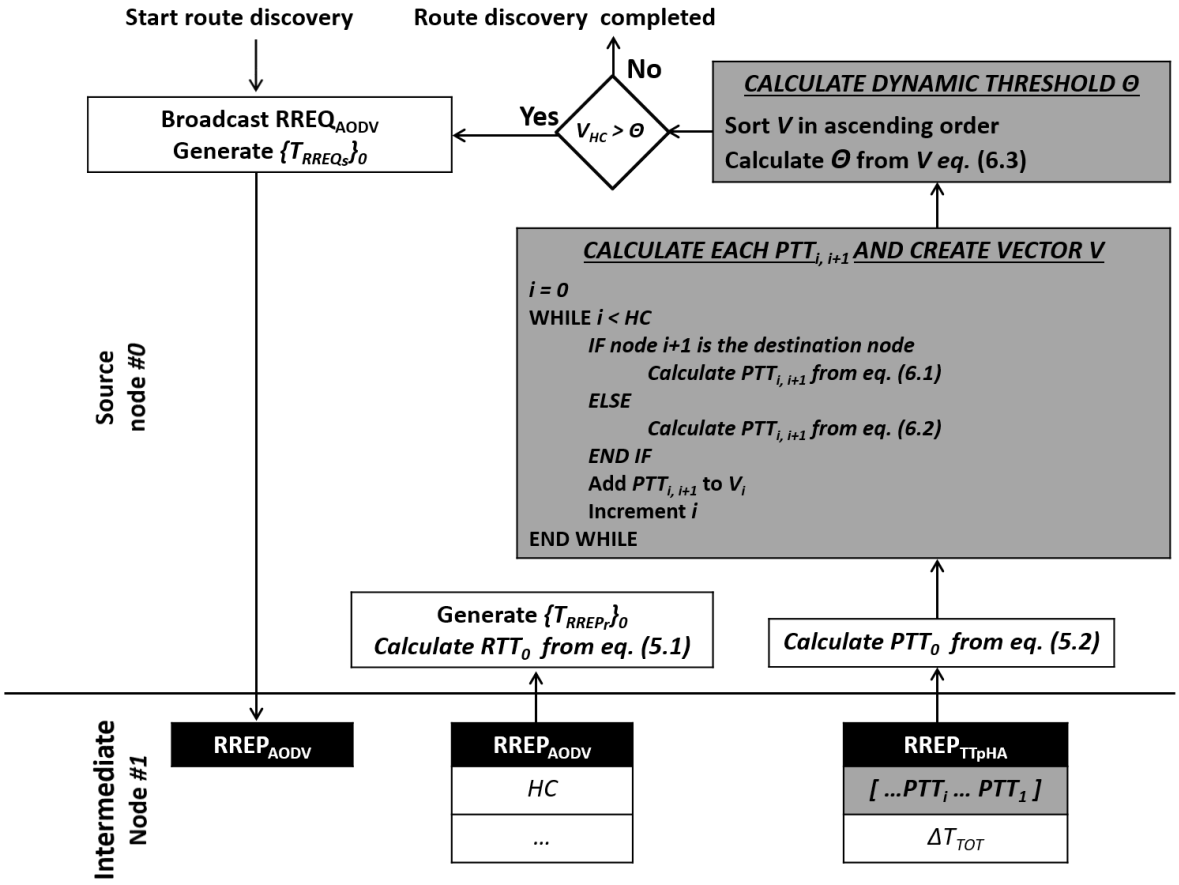

Figure 6.2: Flowchart of the TTpHA algorithm at the source node where the new elements are shaded in grey (other blocks are as for TTHCA (Karlsson et al., 2011)).

6.2.2. Details and Critical Analysis of the Dynamic Threshold Θ

To successfully identify the $PTT_{i,i+1}$ of a wormhole link it must be compared with a threshold value that is considered to be the upper bound of a range of healthy hop packet traversal time values. Other packet delay approaches such as TTM, WAP, M-TTM, and TTHCA use static thresholds for this purpose, e.g. in M-TTM the maximum permissible $PTT_{i,i+1}$ is set to 1 µs while in TTHCA the corresponding maximum permissible PTT/HC is defined in eq. (5.3). Using a fixed threshold is fine provided some specific network conditions are upheld, i.e.

outdoor LOS environments. When moving indoors however, the momentary radio range R_i at each node will incur variations due to physical obstacles between nodes and R may not necessarily be constant on all devices because of different types of hardware, such as antennae. To automatically adapt to variable network environments and diverse node hardware, the Θ threshold value applied in TTpHA needs to be dynamically determined. To achieve this, an outlier detection technique, such as Grubb's test (Grubbs, 1969), the Box plot method (Tukey, 1977), or Dixon's Q-test (Dean & Dixon, 1951) needs to be applied to identify the probable hop packet traversal time value $PTT_{i,i+1}$ of a wormhole link, which is typically significantly higher than any healthy $PTT_{i,i+1}$. To define the threshold Θ, the Q-test was chosen due to its ease of implementation, low computational complexity and being specifically designed for small sample numbers n, typically $3 \leq n \leq 10$. While larger sample numbers ($n \leq 30$) were considered (Rorabacher, 1991), it is a pragmatic design assumption that $n \leq 30$ since at higher values, communicating nodes will be located unrealistically long distances apart so any route will incur high delays. In contrast, the Grubb's test is not recommended for $n < 7$ and the Box plot method requires $n > 4$ in order to produce reliable results. The Q-test was thus a logical choice for this purpose since in analyzing all $PTT_{i,i+1}$ values of a route, then n = HC. If a route is infected by a PM wormhole, then the minimum HC for that route will be 3 i.e., the route comprises only the destination node and the malicious wormhole pair. When HC = 3 for a wormhole infected route, then one of the hops must include the wormhole link and this will exhibit a higher $PTT_{i,i+1}$ value than the two legitimate hops. In applying the Q-test, an unrealistically high $PTT_{i,i+1}$ value is identified if:

$$\frac{V_n - V_{n-1}}{V_n - V_1} > Q_C \tag{6.3}$$

where V_n and V_{n-1} is the largest and second largest $PTT_{i,i+1}$ value respectively, V_1 is the smallest value, and Q_C is the critical Q value for a chosen confidence level α and sample numbers n = HC (Verma & Quiroz-Ruiz (2006). Thus, the threshold Θ can be derived from

eq. (6.3) as:

$$\Theta = \frac{V_{n-1} - Q_C V_1}{1 - Q_C} \tag{6.4}$$

If the route HC < 3, then eq. (6.4) cannot be used since such a route cannot include a PM wormhole and it is then reasonable to apply the fixed threshold in eq. (5.2) by defining $\Theta = \frac{R}{S}$. A wormhole is then suspected if

$$V_n > \Theta \tag{6.5}$$

If several wormholes exist in the MANET, then a route can potentially include multiple infected links. If these wormholes are all PM O-B with their respective lengths (r_{wh}) being analogous, then there is a risk that all the wormhole links will go unidentified if only n = HC is considered in both eq. (6.4) and (6.5). Consequently, eq. (6.4) and (6.5) must be repeated for $1 \leq n \leq HC$. The choice of parameter α provides a useful design trade-off mechanism between wormhole and *false positive (FP)* rates. A high α means low *FP rates* but a concomitant low wormhole detection probability. Conversely, a lower α increases the probability of detecting a wormhole, but with a higher *FP rate*. A confidence level α = 0.9 was empirically determined for all the ensuing simulations as it represents the best design choice from a detection perspective.

A critical analysis of how key framework factors including radio range variability, timestamp resolution, and node mobility, influence the wormhole detection capability of Θ will now be presented.

Radio Range Variability

If the route $HC \geq 3$, then eq. (6.4) is applied to calculate Θ. As Θ is automatically determined from all the values in V, the TTpHA wormhole detection performance is dependent not only on the calculated hop packet traversal time value $PTT_{i,i+1}$ of the wormhole link as in the static

threshold scenario, but also on the variability of $V_{1\ldots n-1}$. The maximum permissible variability of $V_{1\ldots n-1}$ which can still guarantee 100% detection of PM O-B wormholes is defined by the following *Lemma*.

Lemma 6.1: If V_n has a high $PTT_{i,i+1}$ as a result of a wormhole, then it will always be detected provided all $V_{1\ldots n-1}$ values are bounded by:

$$\frac{xr_{wh}}{S} \leq V_i \leq \frac{R}{S} \tag{6.6}$$

where x defines the smallest permissible hop distance $r_{i,i+1}$ in relation to r_{wh}, derived from eq. (6.3) as:

$$\frac{r_{wh} - R}{r_{wh} - x \cdot r_{wh}} = Q_C \Longrightarrow x = \frac{r_{wh}(1 - Q_C) - R}{R(-Q_C)} \tag{6.7}$$

for the worst case scenario being $V_{n-1} = \frac{R}{S}$, i.e. when the largest $r_{i,i+1} = R$.

Proof: If $V_{n-1} = \frac{R}{S}$ and $V_1 \geq \frac{xr_{wh}}{S}$ then from eq. (6.4) $\Theta < \frac{r_{wh}}{S}$ and thus the wormhole is detected. Correspondingly, if $V_1 < \frac{xr_{wh}}{S}$ then $\Theta \geq \frac{r_{wh}}{S}$ and the wormhole will not be detected.

■

For example, if R = 250 m, $r_{wh} = 3R$ (3-hop wormhole), and route HC = 3, which means $Q_c = 0.885$ (Verma & Quiroz-Ruiz, 2006), then from eq. (6.7) $x = 0.247$. This means in practice that the distances between the healthy nodes can range between 186 m and 250 m, so if for example $V_1 = \frac{186m}{S}$ and $V_{n-1} = \frac{250m}{S}$ then Θ = 2475 ns, while $V_n = \frac{750m}{S}$ = 2500 ns and thus the wormhole will be detected with a narrow tolerance. Now if for the same example, $V_1 = \frac{185m}{S}$ then Θ = 2501 ns and the wormhole will go undetected. The tolerance of variability in V_i values is dependent on both the route HC and the length of the wormhole. It has been observed in the simulations that when $r_{wh} < 3R$ then it does not attract a significant amount

of network traffic and so it can be pragmatically considered as the shortest possible wormhole link. A range of *x*-values in eq. (6.7) under different wormhole lengths and route HC are plotted in Figure 6.3.

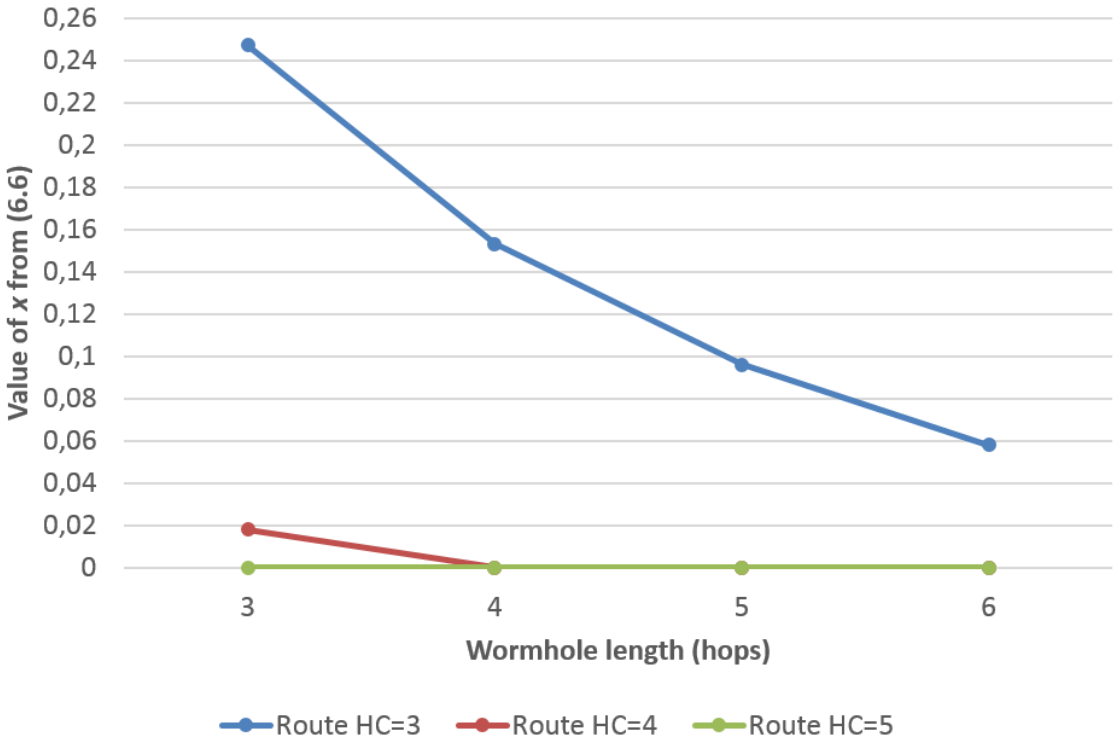

Figure 6.3: Values for *x* calculated from eq. (6.7) for variable route HC and wormhole lengths.

The calculated *x*-values show that all PM wormholes will be detected provided the $HC > 4$ since then all *x*-values are 0 which implies, that all V_i values lie in the range $[0, \frac{R}{S}]$ and the wormhole is detected. Also, if the route $HC = 4$, all PM wormholes ≥ 4 hops will be detected. The most challenging detection scenario for applying Θ is when a PM wormhole infected route $HC = 3$ and the wormhole link is also 3 hops. In these circumstances, if $V_{n-1} = \frac{R}{S}$ then the wormhole will go undetected if $V_1 < \frac{0.247 r_{WH}}{S}$ according to eq. (6.6) and (6.7).

Lemma 5.1 proved that $r_{i,i+1}$ in a homogeneous LOS MANET environment can lie within the range $[0, R]$. This means that TTpHA cannot achieve 100% detection of PM O-B wormholes if both the wormhole link and route are short. Though in real world large scale LOS MANET

environments, where nodes are uniformly distributed, the average $r_{i,i+1}$ value will generally be much closer to the maximum radio range *R*. For example, physical obstacles in network environments and differences in antenna capabilities lead to a higher variability in $r_{i,i+1}$ since the maximum momentary radio range R_i at many nodes is less than *R*. The corresponding bounds for the hop distance $r_{i,i+1}$ in a non-LOS environment are given in the following *Lemma*.

Lemma 6.2: If the maximum radio coverage of a specific node in a non-LOS environment is R_i then the hop distance $r_{i,i+1}$ is bounded by

$$r_{i,i+1} + r_{i+1,i+2} > \min\{R_i, R_{i+1}\} \tag{6.8}$$

$$r_{i,i+1} \leq R_i \tag{6.9}$$

Proof: Eq. (6.8) cannot be false because then the 2-hop neighbour of node #*i* (#*i+2*) would still lie within radio range and thus become a direct (1-hop) neighbor. Correspondingly, eq. (6.9) must be true as otherwise nodes #*i* and #*i+1* will be out of radio coverage. ■

Thus, from *Lemma 6.2* it is evident, that a short PM O-B wormhole in a short route will have a higher probability of being undetected in a non-LOS environment than in a LOS environment. This case will be thoroughly studied in the simulation results presented in the next Section.

Timestamp Resolution (TR)

So far, the ideal case TR = 1 ns has been considered. However, for most off-the-shelf wireless hardware TR > 1 ns and most current technology supports only *TR* = 1 μs (Geiger, 2010), though more specialised devices claim higher resolutions (Microsemi, 2013). The impact of different timestamp resolution levels will now be critically analysed. In TTpHA,

each $PTT_{i\,i+1}$ measurement is calculated from a number of time stamps. Each intermediate node records four timestamps in calculating ΔT_i ($\{T_{RREQr}\}_i$, $\{T_{RREQs}\}_i$, $\{T_{RREPr}\}_i$ and $\{T_{RREPs}\}_i$), while the destination node correspondingly records two ($\{T_{RREQr}\}_i$ and $\{T_{RREPs}\}_i$). The source node also records two time stamps in calculating RTT namely $\{T_{RREQs}\}_i$ and $\{T_{RREPr}\}_i$. The measurement error due to the timestamp resolution (E_{TR}) for each individual recorded timestamp lies within the bounds:

$$0 \leq E_{TR} < TR \tag{6.10}$$

The value of each recorded timestamp can therefore be expressed as

$$\{T_{RREQs}\}_i = \{T_{RREQr}\}_i = \{T_{RREPs}\}_i = \{T_{RREPr}\}_i = T_A + E_{TR} \tag{6.11}$$

where T_A is the actual time of arrival of the first bit of an incoming or actual transmission time of the first bit of an outgoing routing packet. For example, TR = 1 μs means that the wireless hardware is capable of registering an event, i.e. the arrival of the first bit of an incoming or transmission of the first bit of an outgoing packet, not more frequently than once every 1 μs. If the hardware checks for an event at time T_C and the actual time of the event is for example, $T_A = T_C$+0.5 μs, then the event will be registered and a time stamp recorded at T_C+TR, so E_{TR}=$(T_C$+$TR) - T_A$. Conversely, if $T_A = T_C$ then $E_{TR} = 0$, but as this is a causal system, E_{TR} must be positive because an event cannot be registered before it has occurred. Using eq. (6.10) and (6.11), the variability caused by E_{TR} in each of the measured $PTT_{i\,i+1}$ values is given by the following *Lemma*.

Lemma 6.3: Assuming a uniform distribution for E_{TR}, then each measured $PTT_{i,i+1}$ value lies within the following bounds:

$$\left(\frac{r_{i,i+1}}{S} - max(E_{TR})\right) \leq PTT_{i,i+1} \leq \left(\frac{r_{i,i+1}}{S} + max(E_{TR})\right) \tag{6.12}$$

where $max(E_{TR})$ is the maximum E_{TR} value within the range specified by eq. (6.10).

Proof: Since each $PTT_{i,i+1}$ can be expressed as:

$$PTT_{i,i+1} = \frac{\{T_{RREPr} - T_{RREQs}\}_i - \{T_{RREPs} - T_{RREQr}\}_{i+1}}{2} \quad (6.13)$$

it is evident E_{TR} gives the smallest possible $PTT_{i,i+1}$ as $E_{TR} = max(E_{TR})$ when generating $\{T_{RREQs}\}_i$ and $\{T_{RREPs}\}_{i+1}$, while $E_{TR} = 0$ for all other timestamps. In this scenario $PTT_{i\,i+1}$ will be close to the lower bound in eq. (6.12). Conversely, the highest possible $PTT_{i,i+1}$ occurs as $E_{TR} = max(E_{TR})$ when generating $\{T_{RREPs}\}_i$ and $\{T_{RREQr}\}_{i+1}$, with $E_{TR} = 0$ for all other timestamps, which results in $PTT_{i,i+1}$ being close to the upper bound in eq. (6.12). ■

Using eq. (6.10 – 6.11) and *Lemma 6.3*, it can be concluded that a PM O-B wormhole will always be detected provided the following condition is upheld:

$$\left(\frac{r_{wh}}{S} - max(E_{TR})\right) > \frac{\left(\frac{max(r_{i,i+1})}{S} + max(E_{TR})\right) - Q_C(\frac{min(r_{i,i+1})}{S} - max(E_{TR}))}{1 - Q_C} \quad (6.14)$$

Rearranging this equation gives:

$$TR < \frac{Q_C(min(r_{i,i+1}) - r_{WH}) + r_{WH} - max(r_{i,i+1})}{2S} \quad (6.15)$$

To illustrate the conditions in eq. (6.14) and (6.15), consider the 5 HC route infected with a PM O-B wormhole shown in Figure 6.4 where A is the source node and D is the destination node. If for example R = 250 m reflects an outdoor environment for IEEE 802.11n compliant hardware, $r_{A,B}$ = 50 m, $r_{B,M1}$=$r_{M2,C}$ = 100 m, $r_{C,D}$=R, and r_{wh} = 750 m (i.e. a 3-hop wormhole), then eq. (6.15) indicates that the TR can be up to 182 ns and the wormhole is still detected with 100% probability. On the other hand if TR = 183 ns, eq. (6.15) is not upheld and as a result the wormhole goes undetected. For a longer wormhole link, e.g. 5 hop, then a larger

TR value can be tolerated, i.e. 551 ns. The TR tolerance is also dependent on the route HC since the wormhole detection performance of TTpHA improves with the number of measurement samples, as shown in *Lemma 6.1*. Using the same $min(r_{i,i+1})$ and $max(r_{i,i+1})$ values in the above example, the corresponding maximum tolerable TR values would be 501 ns (3-hop wormhole) and 1097 ns (5-hop wormhole) if the route HC is as large as 15. It needs to be stressed that eq. (6.14) and (6.15) represents the worst case scenario where the $PTT_{i,i+1}$ of the wormhole link obtains a value close to the lower bound defined in eq. (6.12). In contrast, when its value is close to the upper bound the likelihood for wormhole detection increases, so TTpHA provides satisfactory wormhole attack detection performance even for higher TR values than specified in eq. (6.15), as will be confirmed in the next Section.

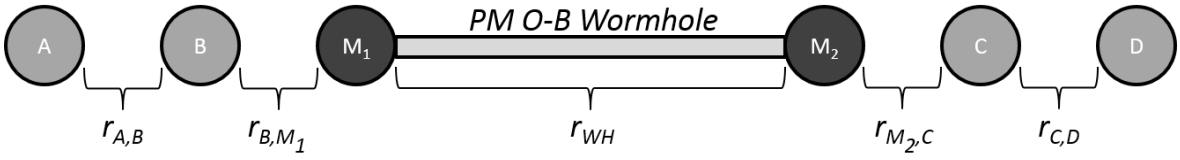

Figure 6.4: An example of a PM O-B wormhole infected route

Mobility

Node mobility during the route discovery procedure will have impact on a measured hop packet traversal time value $PTT_{i,i+1}$ in the sense that it will not exactly correspond to the hop distance value $r_{i,i+1}$ when at some time instant, node #*i* either sends a RREQ or receives a $RREP_{AODV}$, unless of course, both nodes #*i* and #*i+1* are moving in the same direction at the same speed. $PTT_{i,i+1}$ will still represent a valid $r_{i,i+1}$ that lies within the bounds specified by *Lemma 6.2* because even though two successive nodes on a route are moving they are unable to communicate if $r_{i,i+1} > R_i$. For this reason, the wormhole attack detection performance of TTpHA will not be affected. In the next Section, the detection performance of TTpHA will be rigorously evaluated.

6.3. Simulation and Results Analysis

A series of experiments were undertaken to critically analyse the performance metrics, i.e. the wormhole *detection rate* eq. (4.1) and the *FP rate* eq. (4.2), for different wormhole lengths, R_i variations, and TR values. The impact of node mobility on wormhole attack detection performance was also evaluated. The simulation environment used for these experiments, with relevant parameters and applied mobility model, was detailed in Chapter 4. TTHCA (Karlsson et al., 2011) and M-TTM (Qazi et al., 2013) were used as comparators, because TTpHA is an extended version of TTHCA and uses a similar packet delay analysis scheme as M-TTM. As discussed in Chapter 3, the proposed 2 ms fixed threshold for the maximum permissible difference between any measure hop round trip time vlaue $RTT_{i,i+1}$ and *expected* $RTT_{i,i+1}$ is not feasible for PM O-B wormhole detection. Therefore, a wormhole is suspected if a measured $RTT_{i,i+1} >$ *expected* $RTT_{i,i+1}$ in these experiments. Both an outdoor and an indoor MANET environment is considered, with the respective parameter settings being defined in Table 6.1.

Table 6.1: Specific simulation parameter settings used for outdoor and indoor environments.

Parameter	Outdoor settings	Indoor settings
Number of nodes (N)	300	300
Network width (W)	1000 m	100 m
Netowrk length (L)	4000 m	400 m
Maximum radio range *(R)*	250 m	70 m
Number of infected (N_{IR}) and healthy route samples (N_{HR})	200	200

In both environments, it is assumed all nodes use IEEE 802.11n compliant wireless hardware which determines the corresponding R values in Tables 6.1 (Barker et al., 2015). The same outdoor environment dimensions and value of N are used as in Chapter 5 (Jen et al., 2009), while the indoor environment dimensions were chosen to reflect a large building. In a real MANET, the momentary radio range R_i will be dependent on the antenna used and node surroundings. For example, in an indoor environment containing obstructions like walls, R_i

will be smaller than when the node is located in a direct LOS. To reflect the different surroundings and variations in node hardware, a random R_i distance value lying in the range $min(R_i) \leq R_i \leq R$ is introduced. The results from these experiments will be presented in the following subsections.

6.3.1. Variable Radio Range

In the first set of experiments, the comparative detection performance of TTpHA, TTHCA, and M-TTM were evaluated for different levels of R_i variability and wormhole lengths. The results shown in Figure 6.5, reveal that radio range variability for TTpHA, does not negatively impact upon the wormhole detection performance in the way it did for TTHCA, where the combination of a short wormhole link and high radio range variability led to a significant deterioration in the detection rates. In contrast, for TTpHA > 90% of the wormhole infected routes were detected in the outdoor and > 80% in the indoor environment for all tested variations in R_i.

In the outdoor scenario, the wormhole *detection rate* tended to fall with increased R_i variability. For example, the detection rate of the 3-hop wormhole was ≈ 95% for $min(R_i) = R$ and 90% for $min(R_i) = 0.2R$. The opposite trend was observed for the indoor environment, with the wormhole detection rate being 82% in the 3-hop wormhole case for $min(R_i) = R$ and 100% for $min(R_i) = 0.2R$. The reason for this is that the route HC in the indoor environment was often < 5 when $min(R_i) = R$. Hence, the condition in eq. (6.6) has a significantly higher probability of being upheld when $min(R_i) = 0.2R$ since the average route HC is then significantly higher than when $min(R_i) = R$. In the outdoor environment, the average route HC was higher than in the indoor environment and therefore eq (6.6) was mostly upheld even for $min(R_i) = R$.

The detection performance of TTHCA drops dramatically for $min(R_i) < R$ because it is based

on the average PTT/HC and when $R_i < R$ then the average $r_{i,i+1}$ is low in relation to R and so the eq. (5.8) condition does not hold. M-TTM on the other hand, provided 100% detection of all wormholes in the outdoor environment and indoors for 5-hop wormholes but not for wormholes shorter than 5 hop.

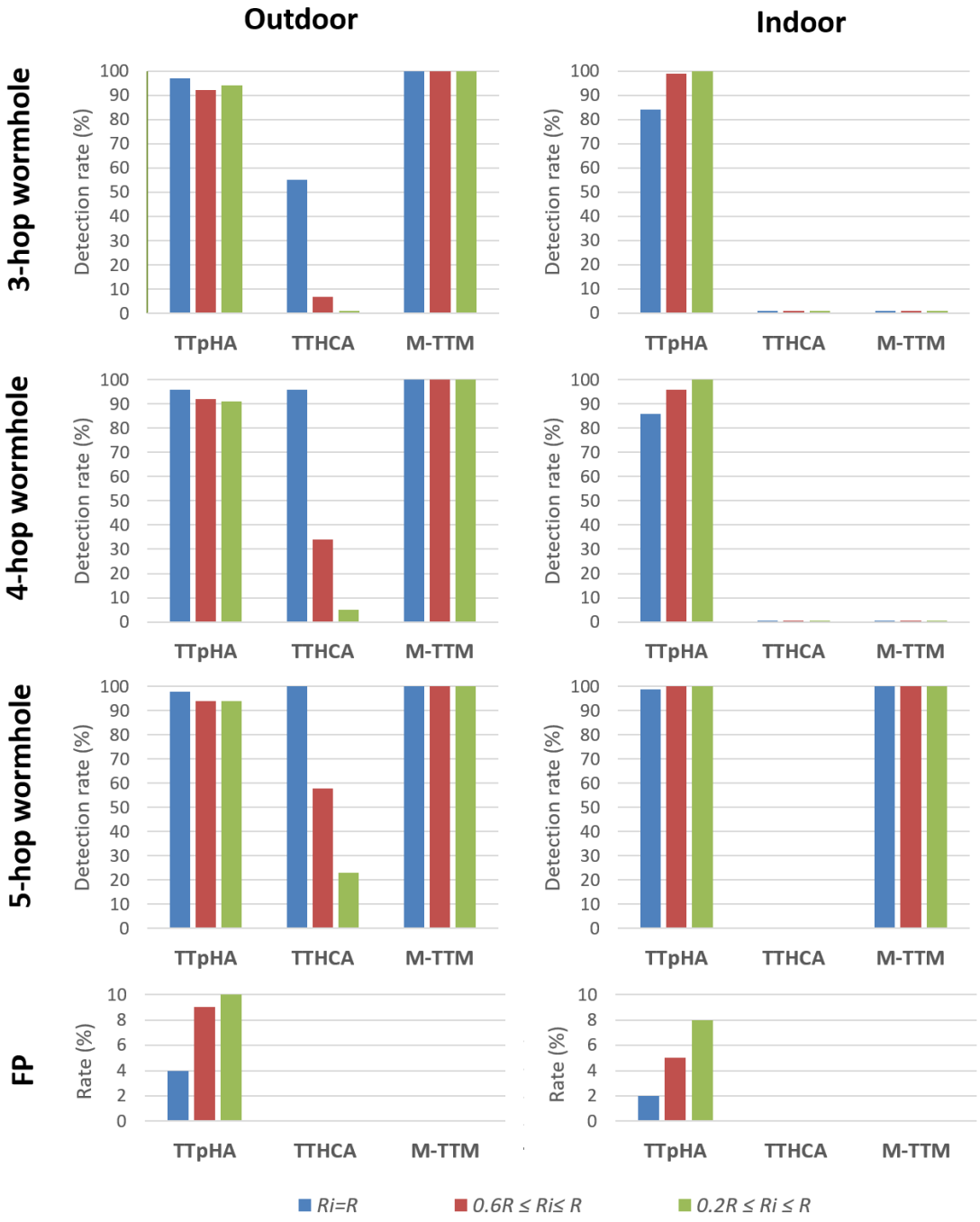

Figure 6.5: Comparative TTpHA and M-TTM wormhole detection and FP performance for different wormhole lengths and radio range variabilities.

The reason is that M-TTM assumes PD_{MAX} = 1 µs when calculating the *estimated* $RTT_{i,i+1}$ (as discussed in Section 3.2.7) and since in these simulations a wormhole is suspected if the measured $RTT_{i,i+1}$ > the *estimated* $RTT_{i,i+1}$ it means that any wormhole link with $r_{wh} > \frac{1\mu s}{s}$ is detected. A cursory analysis of the results reveals that TTpHA is much more flexible since it can automatically adjust its threshold to the prevailing environment while M-TTM and TTHCA are essentially only applicable in outdoor environments.

In terms of the corresponding *FP rates*, it was observed that the level of R_i variability does impact on the performance of TTpHA since in the outdoor environment the *FP rate* was just 4% when all $R_i = R$ while it was 10% when $0.2R \leq R_i \leq R$. The corresponding *FP rates* in the indoor environment were marginally lower at 2% and 8% respectively. These results can be reduced by choosing a higher confidence value α in determining the threshold, however this will decrease wormhole *detection rates*. From a detection perspective, a *FP rate* of up to 10% is still a laudable outcome when cognisance is made of the significant detection improvement achieved by TTpHA compared to both TTHCA and M-TTM. Furthermore, a higher *FP rate* does not mean a node cannot communicate with a destination node, but rather that it simply is unable to use the shortest route.

It needs to be noted that the fixed thresholds used in M-TTM and TTHCA can be manually adjusted to indoor situations to provide similar detection performance to those achieved for outdoor environments. However, since this would involve a decrease in the actual threshold values, M-TTM and TTHCA would at the same time generate a larger number of false positive detections in the outdoor environment. This highlights a key benefit of TTpHA, namely its ability to automatically adapt to its environment and move seamlessly between different surroundings without requiring manual parameter intervention.

These results are based on the assumption that each time stamp used in all three detection

techniques can be recorded with a 1 ns measurement accuracy, which is not a wholly realistic assumption for all constituent MANET hardware. Consequently, the next Section presents a performance insight into relaxing this assumption.

6.3.2. Time Measurement Accuracy

The next series of experiments analysed the requirements imposed upon wireless interface hardware in regard to the timestamp resolution tolerances required to monitor and process in-coming and out-going routing packets. Again different wormhole lengths were used and the performance of TTpHA and M-TTM was tested across a range of TRs from 1 ns to 1 μs, where for example, TR = 10 ns means that every node is capable of both detecting and timestamping reception or transmission of a routing packet every 10 ns. In these experiments, a radio range variability of $0.2R \leq R_i \leq R$ was used to reflect a realistic mixture of node hardware and obstacles. Due its overall poor wormhole detection performance in highly variable radio range scenarios, TTHCA was not included as a comparator in this particular results analysis.

The simulation results shown in Figure 6.6 conclusively prove that TTpHA wormhole detection performance does not significantly decrease in either outdoor or indoor environments. Even for the case TR = 100 ns, more than 90% of all tested wormholes were successfully detected. The reason for this is logical in the outdoor scenario because the maximum allowable TR value in eq. (6.15) >100 ns when the route HC ≥ 5 and r_{wh} = 750 m, while in this environment the majority of the obtained wormhole infected routes had more than 5 hops.

The corresponding maximum tolerable TR value for the indoor environment does not exceed 100 ns before the route HC ≥ 9. However, since each hop packet traversal time value $PTT_{i,i+1}$ can vary within the bounds specified in *Lemma 6.3*, the eq. (6.15) condition is only

compromised in exceptional circumstances, so the wormhole *detection rate* does not significantly decrease even though a large proportion of the wormhole infected routes were shorter than 9 hops.

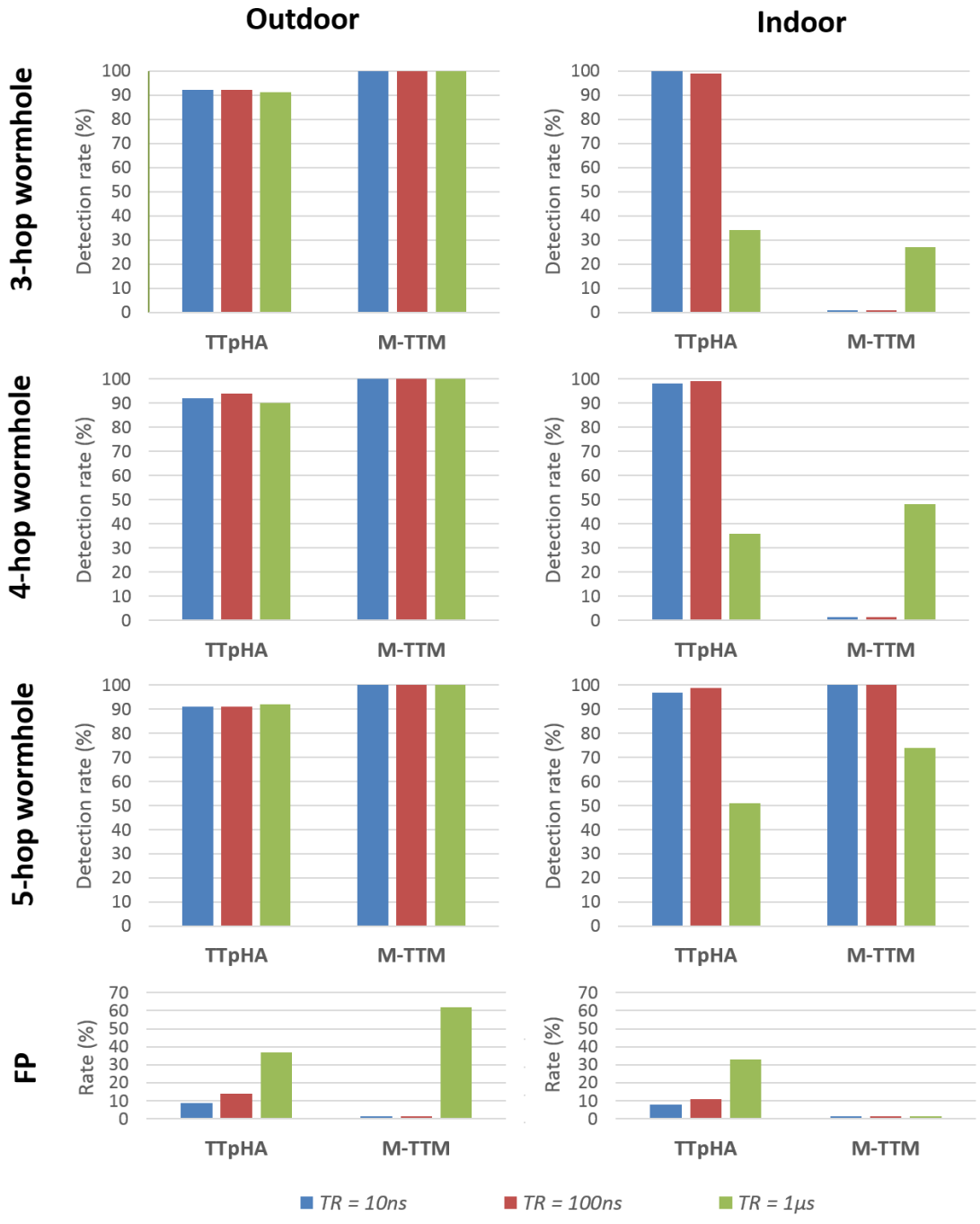

Figure 6.6: Comparative TTpHA and M-TTM wormhole detection performance and FP detections for different wormhole lengths and TR values.

Even when TR = 1 μs, TTpHA still provides good performance in the outdoor environment scenario with a *detection rate* of ≈90% for all wormholes. For the indoor environment, the wormhole detection performance becomes heavily degraded when *TR* = 1 μs with a *detection rate* of only 30-50%. The reason is that TR is in fact larger than any $\frac{r_{i,i+1}}{S}$ as well as $\frac{r_{wh}}{S}$ and therefore it is in practice impossible to discern a healthy from a wormhole infected link which is evidenced by the corresponding *FP rate* (~32%) being akin to the *detection rate*.

When TR = 1 μs, M-TTM interestingly detected nearly 30% of the 3-hop wormholes and up to 50% of the 4-hop wormholes in the indoor environment even though for both wormhole lengths $\frac{r_{wh}}{S} < PD_{MAX}$. The reason for this is that $(PD_{MAX} - \frac{r_{wh}}{S}) < TR$ and as a result E_{TR} often causes a measured wormhole link $PTT_{i,i+1}$ to be $> PD_{MAX.}$ While these are still poor results, the detection rate of the 5-hop wormhole was satisfactory as more than 70% of the wormholes were detected compared to 50% for TTpHA. However, when cognisance is taken of the overall wormhole detection performance, TTpHA is strikingly superior because it offers greater flexibility than M-TTM in detecting all wormholes types at consistently high rates in both indoor and outdoor environments, even when TR =100 ns. In contrast, M-TTM cannot detect 3 and 4-hop wormholes at all, in the indoor scenario.

While the *FP rate* tends to increase for TTpHA with growing TR values, the *rate* never exceeds 13% when $TR \leq 100$ ns in either of the tested environments. This is a satisfactory outcome since there is still an 87% probability of finding the shortest healthy route between the source and destination nodes. When TR = 1 μs the *FP rat*es for the outdoor and the indoor environments are 37% and 32% respectively which although high, are still acceptable since they only marginally exceed the baseline comparator ground truth (30%) established in Chapter 4. This confirms that TTpHA is able to be implemented in outdoor environments

using existing off-the-shelf IEEE 802.11n compliant wireless hardware. In the outdoor environment, the wormhole *detection rate* of M-TTM was, as for TTpHA, unchanged under all tested TR values. However, for TR = 1 µs, M-TTM generated a *FP rate* of 62% which is too high as it means in only 38% of cases can the shortest route be used for communication. The reason for this high *FP rate* is that $\frac{PD_{MAX} - R}{S} = 166$ ns which is much less than TR = 1 µs and therefore there is a high likelihood that the measured $RTT_{i,i+1}$ of a healthy route > the *estimated* $RTT_{i,i+1}$.

So far, it has been assumed that nodes are stationary in both environments during the route discovery procedure. In the next Section this particular assumption will be relaxed.

6.3.3. Mobility

In this set of experiments, the impact of node mobility on wormhole *detection rates* is analysed. The respective comparative results for stationary and moving nodes are displayed in Figures 6.7 and 6.8 for the outdoor and indoor scenarios. The RWM model was chosen for simulating node movement with the maximum velocity assumed to be 33.3 m/s for outdoors and 2.5 m/s for indoors, reflecting the maximum speeds of a car driving along a motorway and walking pace of humans respectively. The results reveal that node mobility does not have any effect on either TTpHA or M-TTM wormhole detection performance in either environment which supports the claim made in Section 6.2. TTpHA false positive detection is slightly increased as a result of mobility in the outdoor environment when TR = 100 ns while the *FP rates* are similar when TR = 1 µs. The reason for this is that node mobility causes higher variability in $PTT_{i\ i+1}$ values which naturally increases the *FP rate*.

On the other hand, when TR = 1 µs the variability in $PTT_{i,i+1}$ caused by measurement errors is significantly higher than variabilities due to mobility and therefore the *FP rate* is not

increased in this case. For M-TTM, the *FP rate* interestingly decreases from 62% to 33% in the outdoor environment when nodes are moving and TR = 1 µs.

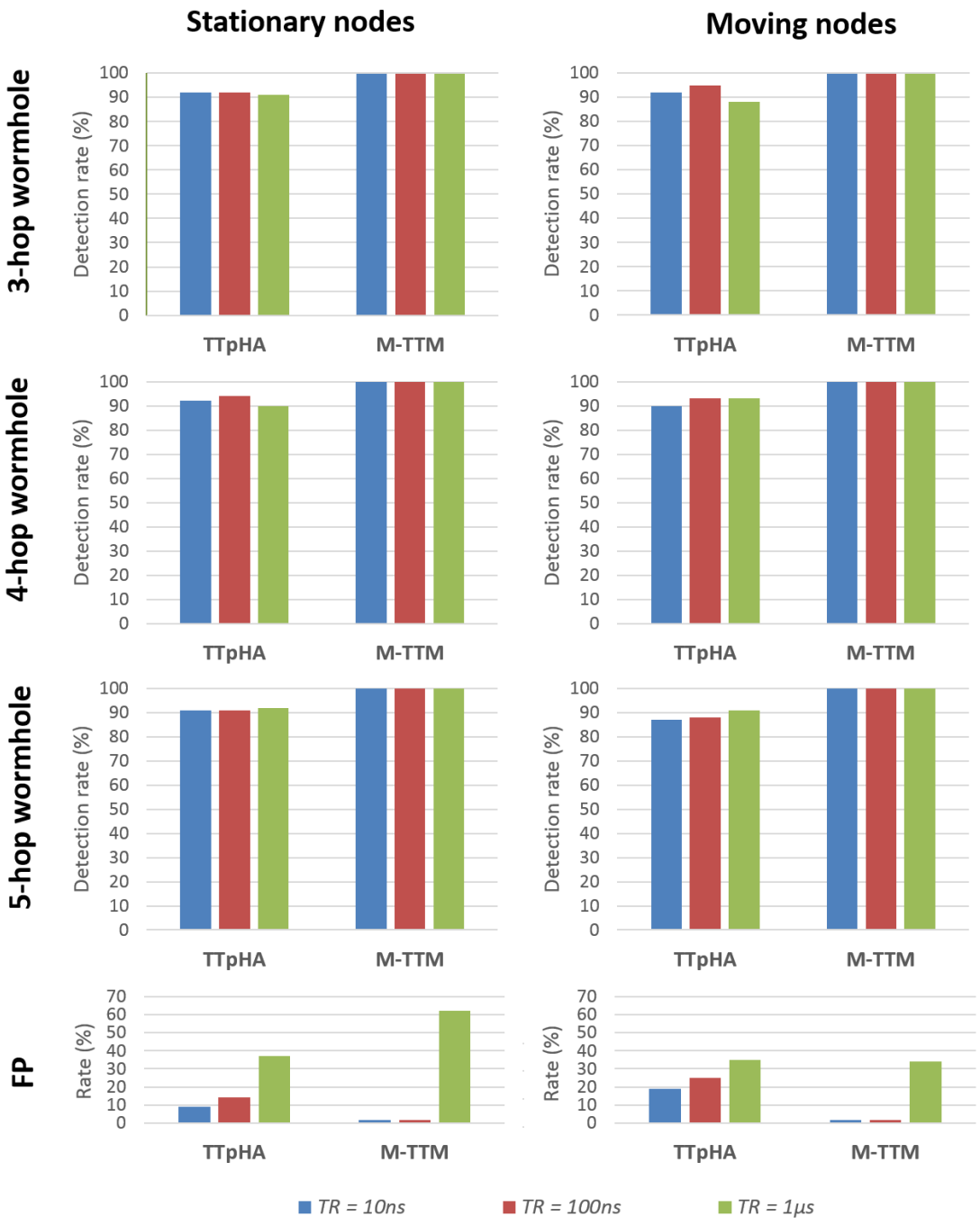

Figure 6.7: Comparative TTpHA and M-TTM wormhole detection performance and FP detections in the outdoor environment for both stationary and moving nodes.

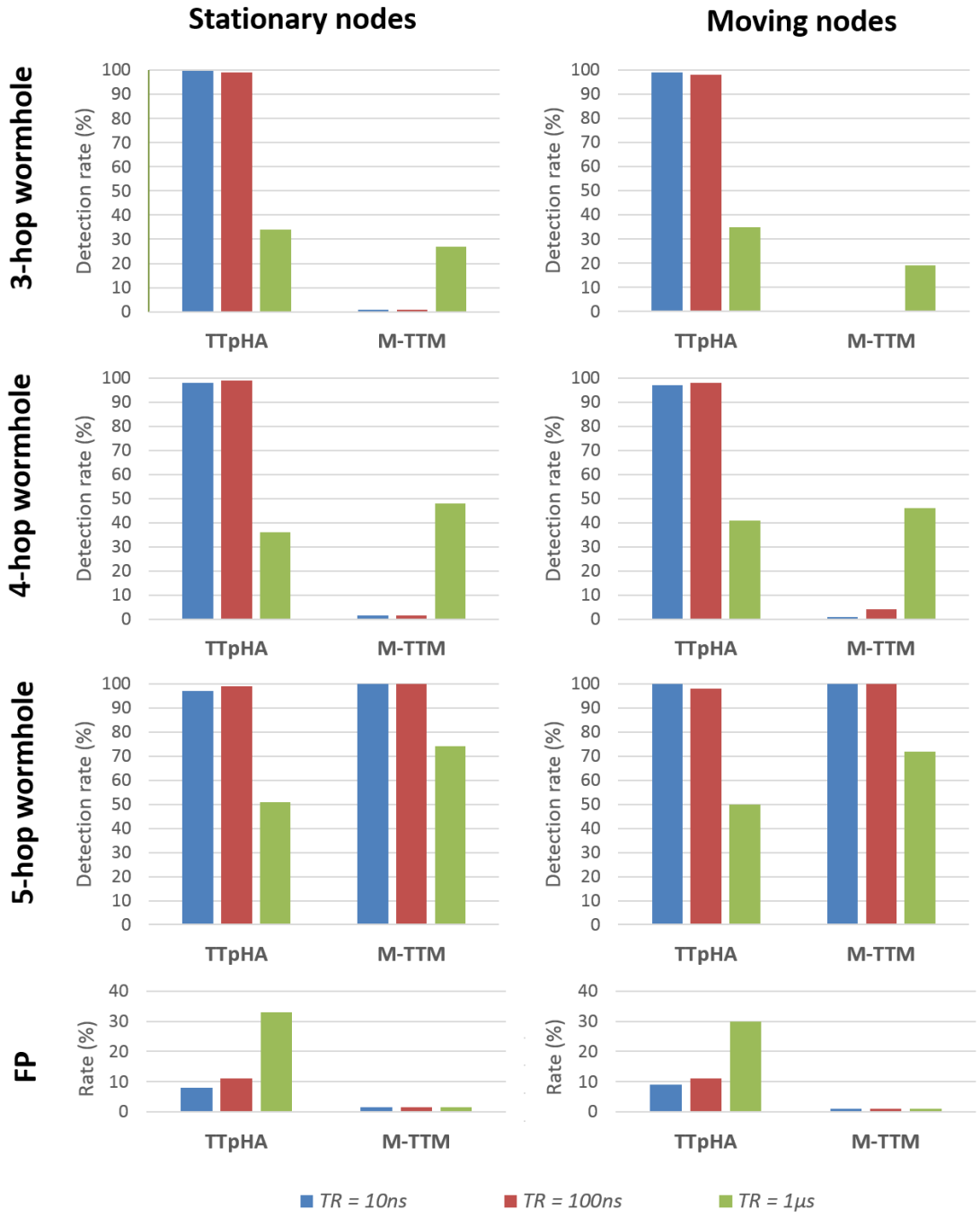

Figure 6.8: Comparative TTpHA and M-TTM wormhole detection performance and FP detections in the indoor environment for both stationary and moving nodes.

The reason is that the $r_{i,i+1}$ on a route tends to decrease when nodes are moving because if $r_{i,i+1}$ between two nodes is close to R they can easily move out-of-range from each other, which breaks the communications link between these nodes even before the route discovery procedure has finished. In the indoor environment, no significant differences were observed in TTpHA and M-TTM *FP rates* since nodes were moving at a significantly lower speed.

6.3.4. Statistical Significance Tests

To assess the statistical significance of the observed differences between TTpHA and TTHCA/M-TTM the *Fisher's exact test* (McDonald, 2014) was applied in a similar manner to that presented in Chapter 5. Again, the rationale behind this test was to statistically determine whether the choice of wormhole detection mechanism is related to the wormhole *detection* and *FP rates*. The hypotheses were defined as follows:

H_0: TTpHA performance = TTHCA/M-TTM performance

H_1: TTpHA performance ≠ TTHCA/M-TTM performance

The detailed significance test results for all test cases are presented in Tables 6.2 – 6.4. The results confirm that the wormhole *detection* and *FP rate* differences observed between TTpHA and TTHCA/M-TTM are statistically significant, i.e. $p(H_0 = true) < 0.05$, in most cases and most importantly, when TTpHA exhibited clear superior performance compared to TTHCA/M-TTM. In the test scenarios were H_0 = true, the observed *detection rates* of both comparative detection algorithms were either identical or only negligible differences were identified i.e. mostly below 3% and in these cases the conclusion could be reasonably made that the performance of both algorithms were equivalent.

Table 6.2: Fisher's exact test results for the variable radio range test cases where *p* is the probability that H_0 is true.

Environment	Wormhole length (hops)	TTpHA *vs.* TTHCA			TTpHA *vs.* M-TTM		
		$R \leq R_i \leq R$	$0.6R \leq R_i \leq R$	$0.2R \leq R_i \leq R$	$R \leq R_i \leq R$	$0.6R \leq R_i \leq R$	$0.2R \leq R_i \leq R$
Outdoor	3	H_0 = false ($p < 0.0001$)	H_0 = false ($p < 0.0001$)		H_0 = false ($p = 0.0301$)	H_0 = false ($p<0.0001$)	H_0 = false ($p = 0.0004$)
	4	H_0 = true ($p = 1.0000$)			H_0 = false ($p < 0.0073$)	H_0 = false ($p < 0.0001$)	
	5	H_0 = true ($p = 0.1231$)			H_0 = true ($p = 0.1231$)	H_0 = false ($p = 0.0004$)	
	FP	H_0 = false ($p = 0.0073$)			H_0 = false ($p = 0.0073$)	H_0 = false ($p < 0.0001$)	
Indoor	3 - 4	H_0 = false ($p < 0.0001$)			H_0 = false ($p < 0.0001$)		
	5				H_0 = true $p = 0.4987$	H_0 = true ($p=1.0000$)	
	FP	H_0 = true ($p = 0.1231$)	H_0 = false ($p = 0.0017$)	H_0 = false ($p < 0.0001$)	H_0 = true ($p = 0.1231$)	H_0 = false ($p = 0.0017$)	H_0 = false ($p < 0.0001$)

Table 6.3: Fisher's exact test results for the variable TR test cases where *p* is the probability that H_0 is true.

Environment	Wormhole length (hops)	TTpHA *vs.* M-TTM		
		TR = 10 ns	TR = 100 ns	TR = 1 µs
Outdoor	3	H_0 = false ($p < 0.0001$)		
	4	H_0 = false ($p < 0.0001$)	H_0 = false ($p = 0.0004$)	H_0 = false ($p < 0.0001$)
	5	H_0 = false ($p < 0.0001$)		
	FP			
Indoor	3	H_0 = false ($p < 0.0001$)		H_0 = true ($p = 0.1579$)
	4			H_0 = false ($p = 0.0197$)
	5	H_0 = false ($p = 0.0301$)	H_0 = true ($p = 0.4987$)	H_0 = false ($p < 0.0001$)
	FP	H_0 = false ($p < 0.0001$)		

Table 6.4: Fisher's exact test results for variable TR under the influence of node mobility where *p* is the probability that H_0 is true.

Environment	Wormhole length (hops)	TTpHA *vs.* M-TTM		
		TR = 10 ns	TR = 100 ns	TR = 1 µs
Outdoor	3	H_0 = *false* ($p < 0.0001$)	H_0 = *false* ($p = 0.0017$)	H_0 = *false* ($p < 0.0001$)
	4 – 5	H_0 = *false* ($p < 0.0001$)		
	FP	H_0 = *false* ($p < 0.0001$)		H_0 = *true* ($p = 0.9163$)
Indoor	3	H_0 = *false* ($p < 0.0001$)		H_0 = *false* ($p = 0.0005$)
	4			H_0 = *true* ($p = 0.3641$)
	5	H_0 = *true* ($p = 1.0000$)	H_0 = *true* ($p = 0.1231$)	H_0 = *false* ($p < 0.0001$)
	FP	H_0 = *false* ($p < 0.0001$)		

6.3.5. Computational and Network Traffic Overheads

The only additional processing costs incurred by TTpHA in comparison with TTHCA and M-TTM are the source node operations relating to the Q-test outlier technique used to calculate the dynamic threshold Θ in eq. (6.4) and the PTT_i calculations performed at the intermediate nodes. This involves determining and ranking $PTT_{i,i+1}$ values which incurs order of time complexities of $O(HC)$ and $O(HC^2)$ respectively, but since HC is a very small value, this is a negligible increase in the overheads. At each intermediate node, PTT_i has to be computed and added to a new RREP packet parameter which is not required in TTHCA. This involves one operation and a $32 \cdot HC_i$ *bits* larger RREP than in TTHCA, where HC_i refers to the HC from the intermediate node #*i* to the destination. While all these operations are also required in M-TTM, with the exception of ranking, the M-TTM PTT_i values are calculated at the source and the corresponding RREP packets are $3 \cdot 32 \cdot HC_i$ *bits* longer than those in TTpHA. So to summarize, as well as being a more flexible wormhole detection solution, TTpHA consistently affords significant performance improvements in comparison

with TTHCA and M-TTM, while incurring a very small cost in computation and network traffic overheads.

6.3.6. Results Discussion

The presented results show that TTpHA significantly improves PM O-B wormhole detection compared to TTHCA especially in the challenging scenarios of either a short wormhole length < 4 hops or when there is high variability in node radio ranges. TTpHA is able to adapt to different environments as the wormhole *detection rate* is almost identical for both test environments, i.e. outdoors (R = 250 m) and indoors (R = 70 m), while both TTHCA and M-TTM worked in only one environment. In this context, TTpHA successfully fulfils research O*bjective 2* and also *Objective 1* to a higher extent than TTHCA because of its enhanced detection performance for short PM O-B wormholes. A summary of the high level characteristics of TTpHA is provided in Table 6.5.

Table 6.5: Summary of desired characteristic and outcomes for TTpHA.

Desirable Characteristics	Summary
100% wormhole detection	Detection rate for PM O-B wormholes =100% for indoor environments when TR = 1 ns and $min(R_i) = 0.2R$. In other test scenarios, detection rate > 90%.
Network topology independent	Detection rate = 100% when the route HC > 5.
No FP	Generally < 10%
Low computational overheads	Complexity is $O(HC)$ or $O(HC^2)$, where HC is a small integer.
Negligible bandwidth load	Routing packet $RREP_{TTpHA}$ introduces a short delay on route discovery and small bandwidth cost for intermediate nodes.
Handles dissimilar node hardware and different network environments	Using a dynamic threshold, variable R or R_i has no impact on detection performance.

A constraint upon TTpHA is if the route HC < 5, then the condition in eq. (6.6) may on some occasions, not hold if there is a high variation in $r_{i,i+1}$.. Therefore 100% wormhole detection is not achieved. While FP detections are generated in all test cases, the defined baseline comparator ground truths for both wormhole *detection rate* (≥ 70%) and *FP rate* (≤ 30%) were still fulfilled by a clear margin in most test scenarios. These restrictions however, are more than offset by the benefits derived from the significant security improvements TTpHA

delivers compared to TTHCA and the state-of-the-art solution M-TTM. A common limitation of both the framework contributions and M-TTM is their inability to detect PM O-B wormholes when low TR hardware is used in indoor environments where radio ranges are short. Some preliminary ideas for possible solutions to this challenging issue will be presented in the Future Work (Chapter 8).

6.4. Summary

This Chapter has presented a new wormhole detection algorithm, TTpHA, which extends TTHCA to significantly improve detection performance by analysing PTT for each hop ($PTT_{i,i+1}$), rather than the average PTT. The most distinguishing feature of TTpHA is its use of a dynamic threshold for the maximum permissible $PTT_{i,i+1}$ which enables TTpHA to adapt to variable radio ranges in diverse environments and dissimilar node hardware. Results confirm that TTpHA performed well in both indoor and outdoor environments, in contrast to the fixed threshold based comparators, TTHCA and M-TTM, which were only effective in the outdoor environment. The assumption for high TR hardware and stationary nodes was relaxed and TTpHA requirements on TR for different environments and the impact of node mobility on the detection performance were critically analysed. It was proven that TTpHA can both tolerate low TR hardware and use off-the-shelf IEEE 802.11n compliant wireless hardware in outdoor environments. So far, it has been assumed all acquired PTT measurements are accurate and have not been fabricated. This assumption will be examined in the next Chapter where the impact of PTT measurement time tampering on TTHCA and TTpHA wormhole detection performance will be rigorously analysed and a novel time tampering detection extension introduced.

7. IDENTIFYING PACKET TRAVERSAL TIME MEASUREMENT TAMPERING

7.1. Introduction

Packet delay based wormhole detection schemes which are based on analysing *packet traversal time* (PTT), such as TTHCA, TTpHA and M-TTM, provide superior wormhole attack detection performance compared to *round trip time* (RTT)-based schemes, but simultaneously bring new security treats related to the time measurements. To be able to calculate route PTT or hop PTT ($PTT_{i,i+1}$), the source node or any intermediate node needs to cooperate with other nodes as PTT is calculated by reducing packet processing times at intermediate nodes from RTT. A potential weakness in this process is that under specific conditions, *participation mode* (PM) wormhole nodes can alter their time measurements and prevent the wormhole from being detected.

In this Chapter, the impact of time tampering attacks on the wormhole detection performance of TTHCA and TTpHA is critically analysed and a novel solution, called *ΔT vector extension* (ΔTVE), is introduced as an extension to TTHCA and TTpHA to identify time tampering in PM *in-band* (I-B) wormholes. ΔTVE replaces the ΔT_{TOT} parameter in the $RREP_{TTHCA/TTpHA}$ packet with a list of the individual routing packet processing delay (ΔT_i) values from all intermediate nodes. A tampered ΔT_i can then be identified by the source node as it will typically be significantly larger than a healthy ΔT_i when the wormhole uses an I-B link. In the next Section the conditions and nature of a time tampering attack will be rigorously analysed before ΔTVE is introduced in Section 7.3.

7.2. The Time Tampering Attack

A wormhole node can potentially prevent TTHCA and TTpHA from detecting infected routes by adding a fictive packet processing time ΔT_F to the ΔT_{TOT} parameter of the

$RREP_{TTHCA/TTPCA}$ packet. It is though important to point out that time tampering is not a modification attack *per se* as the wormhole nodes never alter routing packet parameters, but instead produce false measurement information. Therefore, schemes designed to prevent packet alteration by for example, encrypting all routing packet parameters, will be ineffectual against a TTHCA or TTpHA time tampering attack even though they prevent malicious nodes from tampering with ΔT_i values of the legitimate nodes. The conditions and requirements for launching a successful time tampering attack, from the attackers' point of view, are in TTHCA and TTpHA slightly different due to their distinct time measurement strategies. These will be respectively examined in Sections 7.2.1 and 7.2.2.

7.2.1. Time Tampering in TTHCA

In TTHCA, a wormhole infected route has high PTT/HC and therefore the wormhole nodes must artificially produce a lower PTT than in reality for that route to avoid being detected. This can be accomplished by increasing ΔT_{TOT}. However, since $\Delta T_{TOT} >> PTT$ and ΔT_i values may incur large variations it is challenging for the wormhole nodes to know exactly how to set ΔT_F as it must be precisely defined within a narrow time window to achieve successful time measurement tampering. This window is defined in the following lemma:

Lemma 7.1: Assuming constant *S* and identical *R* for all nodes, then ΔT_F must lie within the following bounds to achieve a successful time tampering attack:

$$\left(RTT - \Delta T_{TOT} - 2HC\frac{R}{S}\right) \leq \Delta T_F \leq (RTT - \Delta T_{TOT}) \tag{7.1}$$

Proof: If ΔT_F is less than the lower bound, TTHCA is still able to detect the wormhole since in this case $\frac{(RTT-(\Delta T_{TOT}-\Delta T_F))/2}{HC} > \frac{R}{S}$ and hence eq. (5.3) is true. Conversely, if ΔT_F is larger than the upper bound, the resulting PTT value calculated at the source node will be negative since then $RTT < (\Delta T_{TOT} + \Delta T_F)$. ■

If the wormhole uses an I-B link, it is not possible for a malicious node to exactly know the time tampering window since it can only be aware of the R and S values in eq. (7.1). However, successful time tampering is still feasible if the malicious nodes (M_1 and M_2) can estimate the RTT of the wormhole link (RTT_{wh}). In an I-B link, RTT_{wh} can have high variations due to the variable packet processing times at nodes through which the wormhole is tunnelled. This makes the precise estimation of RTT_{wh} challenging. One approach for estimating RTT_{wh} for PM wormhole links is to use tightly synchronized clocks at the malicious nodes. During route discovery, wormhole node M_1 adds the exact time information as a parameter within a separate tunnelled packet ($RREQ_{wh}$) after forwarding the RREQ to the other malicious node M_2. Upon receiving $RREQ_{wh}$, M_2 estimates the precise PD of the RREQ through the wormhole PD_{RREQ} by comparing the received time information with its own clock. A similar process occurs when M_2 returns $RREP_{AODV}$ to M_1, with time information this time being added to the tunnelled $RREP_{TTHCA}$ to M_2. When M_1 receives the tunnelled $RREP_{TTHCA}$, it calculates PD_{RREP} to give

$$RTT_{WH} = PD_{RREQ} + PD_{RREP} \tag{7.2}$$

M_1 can then add ΔT_F defined as

$$\Delta T_F = RTT_{WH} - 2\frac{R}{S} \tag{7.3}$$

to ΔT_{TOT} of the $RREP_{TTHCA}$ in addition to its own ΔT_i.

Alternatively, the wormhole nodes can split the time tampering attack into two steps. Firstly, M_2 adds the fictive value

$$\Delta T_{F1} = PD_{RREQ} - \frac{R}{S} \tag{7.4}$$

before M_1 adds

$$\Delta T_{F2} = PD_{RREP} - \frac{R}{S} \tag{7.5}$$

$\Delta T_F = \Delta T_{F1} + \Delta T_{F2}$ is then added to ΔT_{TOT}.

Alternatively, if the wormhole uses an *out-of-band* (O-B) link ΔT_F is easier to estimate provided the wormhole length r_{wh} is known and the PD of the wormhole link is constant. If for example the O-B wormhole link is established using directional antennae, ΔT_F can be estimated as:

$$\Delta T_F = 2(\frac{r_{wh} - R}{S}) \tag{7.6}$$

To illustrate the conditions that must prevail for TTHCA time tampering to be achieved, consider the MANET example in Figure 7.1, where a PM I-B wormhole is formed by nodes M_1 and M_2 which tunnel routing packets between each other via I_2 and I_3.

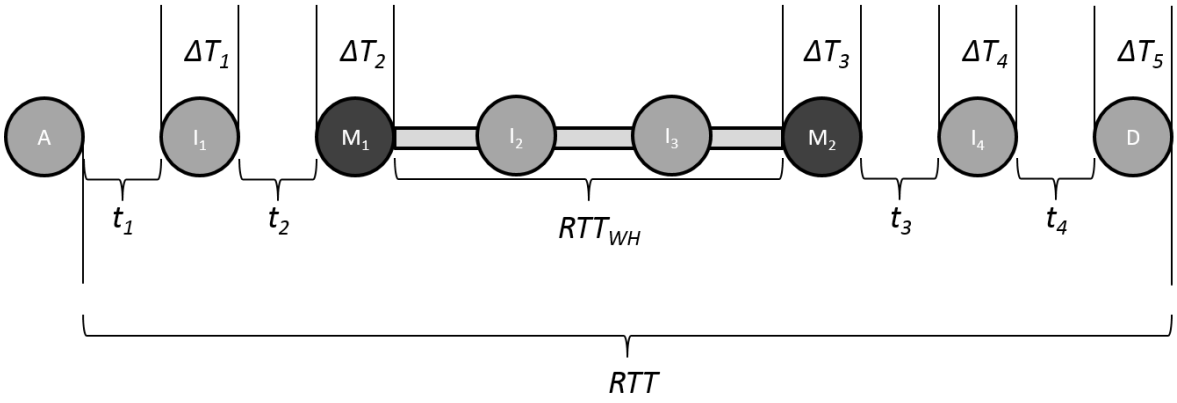

Figure 7.1: MANET scenario where A and D are the source and destination nodes, M_1 and M_2 are malicious wormhole nodes and t_i is $2 \cdot PTT_{i,i+1}$.

It is assumed for simplicity that all nodes are in an idle state, have identical hardware, and the inter-node distance is the same, so both t_i and ΔT_i values are constant. Let t_i = 1600 ns and ΔT_i = 8 ms for all i. If RTT_{wh} = 16.0048 ms then RTT = 56.0112 ms. For this PM I-B scenario, the HC is 5 and ΔT_{TOT} = 40 ms, so from eq. (5.2) source node A calculates PTT =

8.0056 ms giving *PTT/HC* = 1.60112 ms. If it is assumed that R = 250 m, then from eq. (5.3) the upper bound for *PTT/HC* = 833 ns which means TTHCA will successfully detect the wormhole. Using eq. (7.1), it can be determined that M_1 and M_2 are able to prevent detection by increasing ΔT_{TOT} with a value ΔT_F when 16.002867 ms ≤ ΔT_F ≤ 16.0112 ms

This means that the time tampering window is only 8.33 μs wide which is a stringent constraint. However, if synchronized clocks are being used by both M_1 and M_2, it is still a realistic design tolerance in achieving wormhole detection avoidance.

In this PM I-B example, both M_1 and M_2 will calculate ΔT_F = 16.003133 ms which implies that the tampered value falls within the window in eq. (7.1) defined in *Lemma 7.1* to avoid wormhole discovery. In these circumstances, the tampered measurement results in ΔT_{TOT} = 56.003133 ms. From eq. (5.2) the source node A calculates *PTT* = 4.033 ns and *PTT/HC* = 806 ns. This means that this wormhole route will be undetected by TTHCA.

7.2.2. Time Tampering in TTpHA

A wormhole infected route is detected in TTpHA if any hop packet traversal time ($PTT_{i,i+1}$) is larger than the dynamic threshold Θ in eq. (6.4). Malicious nodes must therefore artificially produce a $PTT_{i,i+1} \leq \Theta$ to avoid detection which, as in the case of TTHCA above, is accomplished by increasing $\Delta T_{TOT.}$ Since however, the PTT is analysed for each hop in TTpHA rather than the average PTT as in TTHCA, the time tampering window is narrower than in *Lemma 7.1* and is formally defined as follows.

Lemma 7.2: Assume two malicious wormhole nodes M_1 and M_2 and the next hop node M_3 to M_2 on a route towards the destination node, then ΔT_F must lie within the following bounds to achieve a successful time tampering attack:

$$\left((2PTT_1 - 2\Theta\ ) - 2PTT_2\right) \leq\ \Delta T_F\ < (2PTT_1 - 2PTT_2\ ) \tag{7.7}$$

Proof: $PTT_{1,2} = PTT_1 - \ PTT_2 = \frac{\left((RTT_1 - \{\Delta T_{TOT}\}_2\ ) - (RTT_2 - \{\Delta T_{TOT}\}_3)\right)}{2}$ where $\{\Delta T_{TOT}\}_i$ refers to the ΔT_{TOT} parameter as calculated at node #*i* after it has added its own ΔT_i. So when ΔT_F is added to $\{\Delta T_{TOT}\}_2$, then evidently $PTT_{1,2} > \Theta$ when ΔT_F is less than the lower bound in eq. (7.7). Conversely, if ΔT_F is greater than or equal to the upper bound then $PTT_{1,2} \leq 0$. ■

As Θ is unknown by the malicious nodes, either ΔT_F or ΔT_{F1} and ΔT_{F2} cannot be estimated as in eq. (7.3) or eq. (7.4) and eq. (7.5). Instead, the malicious nodes can use for instance, the PTT_i values in the $\text{RREP}_{\text{TTpHA}}$ packet and then set ΔT_F as:

$$\Delta T_F = RTT_{WH} - \ 2PTT_2 \tag{7.8}$$

when M_3 is the destination node, or otherwise:

$$\Delta T_F = RTT_{WH} - \ 2(PTT_2 - PTT_3) \tag{7.9}$$

The rationale behind this is that since $PTT_{i,i+1}$ is calculated in accordance to eq. (6.1) and (6.2) the malicious nodes can by defining ΔT_F as in eq. (7.8) and (7.9) create the illusion that $PTT_{1,2}$ is equivalent to $PTT_{2,3}$. Correspondingly, to split ΔT_F in two parts, M_2 can set ΔT_{F1} and M_1 ΔT_{F2} as

$$\Delta T_{F1} = PD_{RREQ} - \ PTT_2 \tag{7.10}$$

$$\Delta T_{F2} = PD_{RREP} - \ PTT_2 \tag{7.11}$$

if node M_3 is the destination node, otherwise

$$\Delta T_{F1} = PD_{RREQ} - \ (PTT_2 - \ PTT_3) \tag{7.12}$$

$$\Delta T_{F2} = PD_{RREP} - (PTT_2 - PTT_3) \quad (7.13)$$

In applying either eq. (7.10 and 7.11) or eq. (7.12 and 7.13), M_1 must also decrease PTT_1 by subtracting it with an artificial value PTT_F, otherwise the calculated $PTT_{i,i+1}$ value for the previous hop to M_1 will be negative if RTT_{wh} is high, i.e. the wormhole uses an I-B link . To prevent this, M_1 can set PTT_F for instance as:

$$PTT_F = \frac{\Delta T_{F2}}{2} \quad (7.14)$$

These value selections for PTT_F, ΔT_{F1} andΔT_{F2} create the illusion that $PTT_{1,2}$ (the PTT of the wormhole link) is the same as $PTT_{2,3}$ and so the wormhole goes undetected.

If the wormhole uses an O-B link, ΔT_F is easier to estimate provided the wormhole length r_{wh} is known and the PD of the wormhole link is constant. For such a wormhole, ΔT_F can be estimated analogously to eq. (7.6) with R replaced by either $2(PTT_2 - PTT_3)$ or alternatively $2PTT_2$, if node M_3 is the destination.

To illustrate a scenario where malicious nodes M_1 and M_2 launch a time tampering attack on TTpHA, consider the MANET example in Figure 7.1 again, with t_i = 1600 ns and ΔT_i = 8 ms for all i, PD_{RREQ} = 4.0012 ms and PD_{RREP} = 12.0036 ms. In this example, all relevant node time measurements together with the ΔT_{F1}, ΔT_{F2}, and PTT_F values calculated at the two malicious nodes are presented in Table 7.1, for the both the case of a time tampering attack launched in accordance to eq. (7.12 – 7.14), and where no time tampering occurs.

When there is no time tampering, source node A calculates $PTT_{i,i+1}$ = 800 ns, from eq. (6.1) and (6.2), for all i except $i = 1$ ($PTT_{M1, M2}$) which will be 8.0024 ms. Hence, from eq. (6.4) Θ = 800 ns and the wormhole link will be correctly detected.

Table 7.1: Time measurement values for the Figure 7.1 MANET example scenario with t_i = 1600 ns and ΔT_i = 8 ms for all *i*, PD_{RREQ} = 4.0012 ms and PD_{RREP} = 12.0036 ms.

No time tampering							
Node	RTT_i *eq.* (5.1)	$\{\Delta T_{TOT}\}_i$	PTT_i *eq.* (5.2)	$PTT_{i,i+1}$ *eq.* (6.1)/ (6.2)	ΔT_{F1} *eq.* (7.12)	ΔT_{F2} *eq.* (7.13)	PTT_F *eq.* (7.14)
D	-	8 ms	-	-	-	-	-
I_4	8.0016 ms	16 ms	0.8 µs	800 ns	-	-	-
M_2	16.0032 ms	24 ms	1.6 µs	800 ns	-	-	-
M_1	40.008 ms	32 ms	8.004 ms	8.0024 ms	-	-	-
I_1	48.0096 ms	40 ms	8.0048 ms	800 ns	-	-	-
A	56.00112 ms	-	8.0056 ms	800 ns	-	-	-
Time tampering attack (tampered values in bold)							
Node	RTT_i *eq.* (5.1)	ΔT_{TOT}	PTT_i *eq.* (5.2)	$PTT_{i,i+1}$ *eq.* (6.1)/ (6.2)	ΔT_{F1} *eq.* (7.12)	ΔT_{F2} *eq.* (7.13)	PTT_F *eq.* (7.14)
D	-	8 ms	-		-	-	-
I_4	8.0016 ms	16 ms	0.8 µs	800 ns	-	-	-
M_2	16.0032 ms	**28.0004 ms**	1.6 µs	800 ns	4.0004 ms	-	-
M_1	40.008 ms	**48.0032 ms**	**2.4 µs**	800 ns	-	12.0028ms	6.0014 ms
I_1	48.0096 ms	56.0032 ms	3.2 µs	800 ns	-	-	-
A	56.00112 ms	-	4.0 µs	800 ns	-	-	-

Conversely, if M_2 and M_1 respectively add the fictive values ΔT_{F1} = 4.0004 ms eq. (7.12) and ΔT_{F2} = 12.0028 ms eq. (7.13) to ΔT_{TOT}, and M_1 subtracts PTT_F = 6.0014 ms eq. (7.14) from PTT_1 then all $PTT_{i,i+1}$ = 800 ns and the wormhole link will go undetected. Note this example $\Delta T_F = \Delta T_{F1} + \Delta T_{F2}$ = 16.0032 ms is nearly the same as the corresponding TTHCA value of 16.003133 ms. The corresponding time tampering window for TTpHA is however, much narrower (see *Lemma 7.2*) i.e. 12.0028 ms ≤ ΔT_F ≤ 12.0044 ms using eq. (7.7), with the respective windows for TTpHA and TTHCA being 1.6 µs and 8.33 µs.

In the next Section, a new mechanism for identifying time tampering in PM I-B wormhole detection will be presented before it is critically evaluated in Section 7.4.

7.3. The ΔT Vector Extension (*ΔTVE*)

The previous Section showed that the essential condition for the TTHCA and TTpHA algorithms to be unable to detect a wormhole route is for the malicious nodes to increase ΔT_{TOT} within the strict bounds defined in *Lemmas 7.1* and *7.2*. Any successfully tampered ΔT_{TOT} is always greater than the actual ΔT_{TOT} and this observation provided the motivation for investigating whether the ΔT_{TOT} parameter can be analysed for identifying tampered values. Solely analysing ΔT_{TOT} values will not necessarily identify time tampered wormhole routes because these values usually exhibit high variance. Furthermore, O-B wormhole links only consist of transmission medium propagation delays and so only a very small ΔT_F is required for successful tampering as formally defined in eq. (7.6). Analysing each individual ΔT_i can though lead to acceptable time tampering detection in PM I-B wormhole detection and this strategy is utilized in ΔTVE as will now be introduced.

In ΔTVE, ΔT_{TOT} is replaced by a new ΔT *vector* comprising all measured ΔT_i values. This extension means that some new elements are introduced into the TTHCA and TTpHA route discovery process to support the embedding of this vector. These elements are highlighted in the flowcharts of Figures 7.2 and 7.3 by the shaded blocks. The RREQ broadcast procedures remain as in TTHCA and TTpHA, but instead of using a ΔT_{TOT} parameter, the new ΔT *vector* is included in the $\text{RREP}_{\text{TTHCA/TTpHA}}$ packet by the destination node to which the destination node and each intermediate node inserts its individual ΔT_i as a new element.

If a PM I-B wormhole attack is launched alongside a time tampering attack, at least one of the ΔT *vector* components will be falsely increased in accordance with eq. (7.3 – 7.5) or (7.8 – 7.14). An outlier detection technique can now be applied to identify tampered ΔT_i values within the ΔT *vector*. If a suspicious ΔT_i is identified, TTHCA/TTpHA then requests a new route. On the other hand, if no suspicious ΔT_i is found, then TTHCA/TTpHA continues with

its normal wormhole attack detection procedure. The implementation of an outlier detection technique for identifying a tampered ΔT_i is described in detail in the next Section.

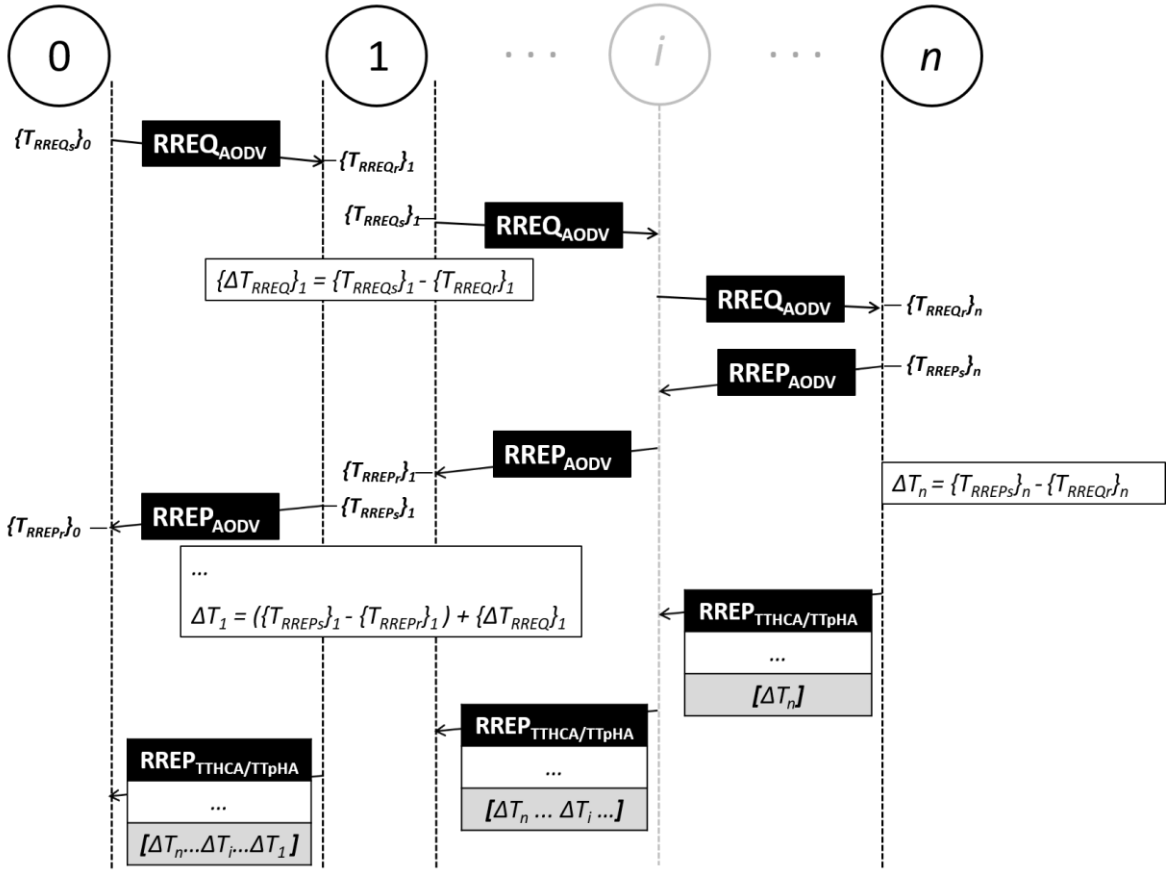

Figure 7.2: The complete TTHCA/TTpHA route discovery procedure with the new ΔTVE elements as shaded blocks.

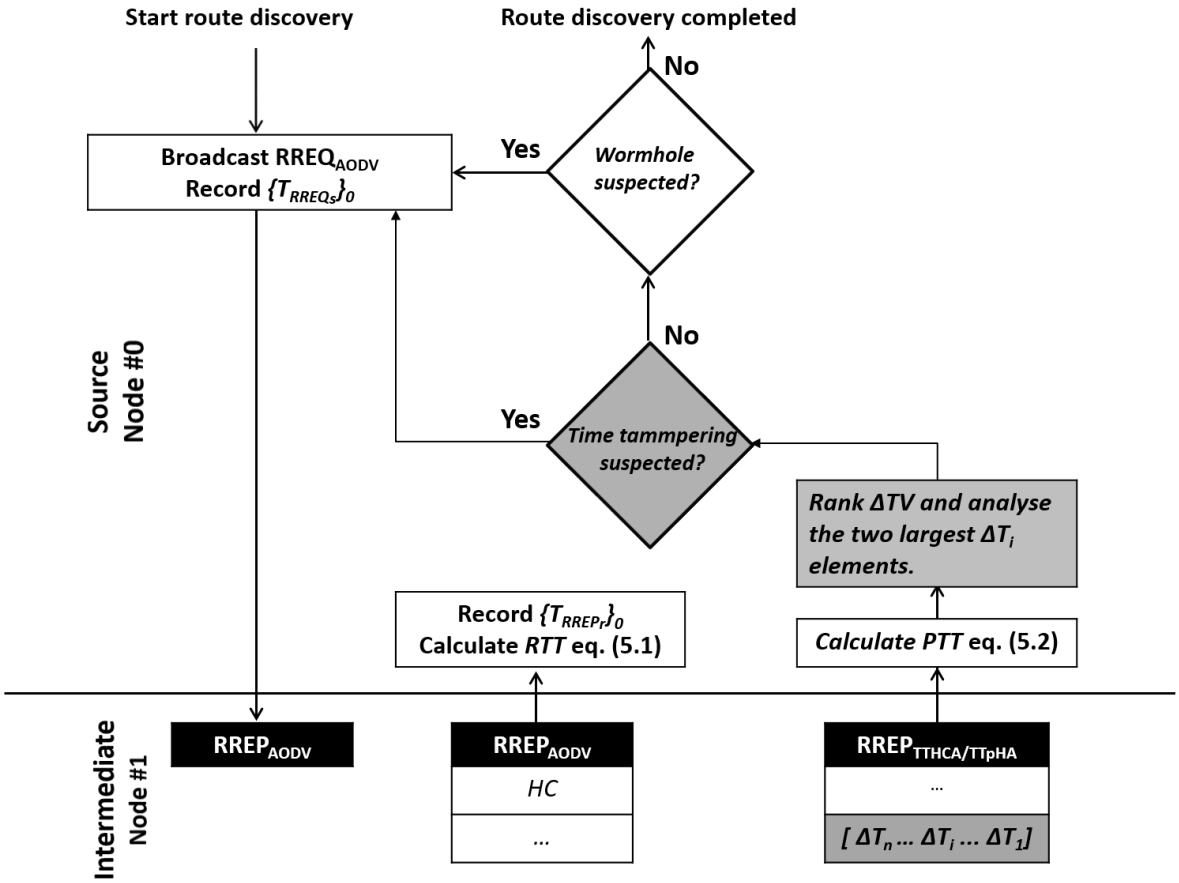

Figure 7.3: The ΔTVE extended TTHCA/TTpHA elements at the source node as shaded blocks.

7.3.1. Identifying Tampered ΔT_i Values

ΔTVE assumes that a malicious node can only modify its own ΔT_i. This is a realistic assumption, since in an actual MANET environment routing packets must be secured from modification attacks for the routing process to be trustworthy. A wormhole link typically consists of two malicious nodes, therefore a ΔT *vector* received through a wormhole infected route will include either one or two tampered ΔT_i values. It is possible to distinguish tampered ΔT_i values from healthy ΔT_i measurements by applying an appropriate outlier detection technique, such as the Grubb's test (Grubbs, 1969), Dixon's Q-test (Dean & Dixon, 1951) or the Box plot method (Tukey, 1977), though several conditions can affect the performance of the chosen outlier method. In this context, two distinct MANET scenarios are considered.

CASE 1: A node has been a part of the network for some time and generated a track record of ΔT_i values gained from ΔT *vectors* in earlier route discovery procedures. In this scenario, the availability of a large number of ΔT_i samples can be reasonably assumed.

CASE 2: A node has joined the MANET for the first time and therefore the only available ΔT_i values are those existing in the ΔT *vector*.

Due to the inherently dynamic nature of a MANET, several different types of ΔT_i distributions can arise which will impact on the performance of the outlier detection scheme. The ideal is when all MANET nodes have identical hardware and the network traffic loads are low. Such a condition would result in negligible ΔT_i variations and time tampering is then straightforward to detect. This is not, however, a realistic MANET situation, because there are a myriad of factors which can cause ΔT_i variations. For example, mixed node processing capacities and packet service times, allied with high network traffic loads in certain parts of the MANET can lead to queuing delays at specific nodes.

In a heterogeneous MANET consisting of uniformly distributed nodes where the network traffic load is low and there are no queuing delays, the ΔT_i values can be assumed to follow a uniform distribution. In MANETs with high network traffic load variations, however, some of the ΔT_i values will include queuing delays which will be much greater than the actual packet service times (Gao & Jäntti, 2004). The ΔT_i values will then tend to follow an assymetric distribution with only a small percentage of ΔT_i values being significantly larger than the average. For such a distribution, it is very challenging to discriminate a tampered from a normal ΔT_i value as a modified ΔT_i can potentially be lower than a healthy ΔT_i if the tampered measurement contains no queuing delay, while the healthy ΔT_i does contain.

The outlier detection method selected for time tampering detection purposes must therefore be applicable to both large and small ΔT_i datasets so that it can cover both CASE 1 and CASE 2 respectively, as well as for both uniform and asymmetric distributed measurements. As in TTpHA wormhole attack detection, Dixons Q-test (Dean & Dixon, 1951) was chosen for this purpose due to its simplicity and applicability to both small and large datasets. Assuming that a route can only be infected by one PM I-B wormhole, the Q-test is used to separately test the two largest ΔT_i values in the ΔT *vector*. The test is performed by first ranking the ΔT *vector* in order and then respectively calculating two Q values:

$$Q_1 = \frac{\Delta T_{HC} - \Delta T_{HC-1}}{\Delta T_{HC} - \Delta T_1} \tag{7.15}$$

$$Q_2 = \frac{\Delta T_{HC-1} - \Delta T_{HC-2}}{\Delta T_{HC-1} - \Delta T_1} \tag{7.16}$$

Time tampering is suspected if either Q_1 or Q_2 is greater than the corresponding critical *Q*-value for the chosen confidence level. In this analysis, a low confidence level of 80% was chosen, since from a security perspective, a higher time tampering detection rate is preferable to a low *FP rate*. The performance of ΔTVE will now be rigorously tested and critically analysed.

7.4. Simulations and Results Analysis

The performance metrics applied for ΔTVE, i.e. the *detection* and *FP rates* in eq. (4.1) and eq. (4.2) respectively, were analysed in the test environment using a customised *ns-2* plugin that simulates different $\{\Delta T_{RREQ/RREP}\}_i$ values as described in Chapter 4. The basis for the plugin was to be able to evaluate ΔTVE under a variety of conditions from a packet processing delay variability perspective, by providing an option to define different variation levels in packet service times T_S and node traffic loads ρ when synthesising the processing delay of a RREQ/RREP packet at each node ($\{\Delta T_{RREQ/RREP}\}_i$). In generating these values, each node is

assumed to have an OS that supports multi-programming, with a scheduler assigning equal time slices to each process in rotation. Thus a logical processor, with the capacity being the ratio of the physical processor capacity and the multi-programming level, executes each multi-programmed task in rotation. Nodes typically have different physical processing capacities and multi-programming levels, but the equivalent multi-programming level for each node will be relatively stable during a single route discovery procedure. The T_S values of the RREQ and RREP packets are thus assumed to be the same at every node, while T_S amongst different nodes is assumed to be variable. Many concurrent route detection procedures lead to routing packet queues in MANET nodes, since received routing packets must be sequentially processed to uphold route table updating requirements. For this reason, the packet processing times ($\{\Delta T_{RREQ/RREP}\}_i$) have been generated using the M/D/1 queuing model (Gross et al., 2008), which assumes Poisson distributed packet arrivals, deterministic T_S, a single central processing unit, and an infinite maximum queue length. Hence, at each node

$$\{\Delta T_{RREQ}\}_i = \{\Delta T_{RREP}\}_i = queuing\ delay + T_S = \frac{T_S(2 - \rho)}{2(1 - \rho)} \tag{7.17}$$

Variations in both node processing capacity and multiprogramming level are reflected by using random T_S values from a uniform probability distribution of different intervals denoted by the *relative standard deviation* (σ_R), which is the standard deviation of all the packet service times divided by their average. Variable network traffic loads between nodes are mirrored by randomly selecting ρ on each node within the interval $0 \leq \rho \leq \rho_{max}$, where ρ_{max} is the maximum network traffic load per node.

Both CASE 1 and CASE 2 scenarios were considered with time tampering attacks simulated in accordance with eq. (7.4) and (7.5). Note the results presented relate solely to the ΔTVE time tampering detection performance which will be identical for both TTHCA and TTpHA

algorithms, while the specific simulation parameters used for these tests are the same as those defined in Table 5.1. This reflects an outdoor environment, though the type of environment in terms of radio ranges in this case is irrelevant, as ΔTVE only analyses ΔT_i values. No comparators' solutions are included since ΔTVE is the only mechanism that specifically addresses this type of time tampering attack, so the baseline ground truths established in Section 4.4 are employed in this analysis. The ΔTVE time tampering performance will now be tested separately for the CASE 1 and CASE 2 scenarios.

7.4.1. CASE 1: MANET Nodes with ΔT_i Track Records

In the first series of experiments, the situation where a node has been in the MANET for a period of time is analysed and there is a history of at least 15 previous ΔT_i values available. Figure 7.4 shows the impact of variations in both routing packet service time (σ_R) and network traffic load (ρ_{max}) upon the time tampering detection performance for different wormhole lengths. The results reveal that for the ideal case where ΔT_i is constant, reflecting nodes having identical hardware and multiprogramming level ($\sigma_R = 0$) and each node carries negligible network traffic load ($\rho_{max} = 0$), then 100% time tampering detection is achieved for all wormhole lengths with no corresponding false positives being detected (see Figure 7.5). Predictably, as variations in ΔT_i increase, the time tampering *detection rate* falls and the *FP rate* increases, though the *detection rate* is still at least 86% for all wormhole lengths analysed even when $\sigma_R = 0.35$ and $\rho_{max} = 0.6$.

For wormhole lengths ≥ 5 hops, 87% of tampered ΔT_i values are successfully detected under all conditions when $\sigma_R = 0.5$ and $\rho_{max} = 0.9$. A notably aspect of the performance of ΔTVE, is that a minimum of 74% of tampered ΔT_i values can still be detected even when the wormhole length is 4 hops. Pragmatically, this means that successfully launching a time tampering attack in wormholes greater than 4 hops will be extremely difficult to achieve since the probability of avoiding detection is less than 30%.

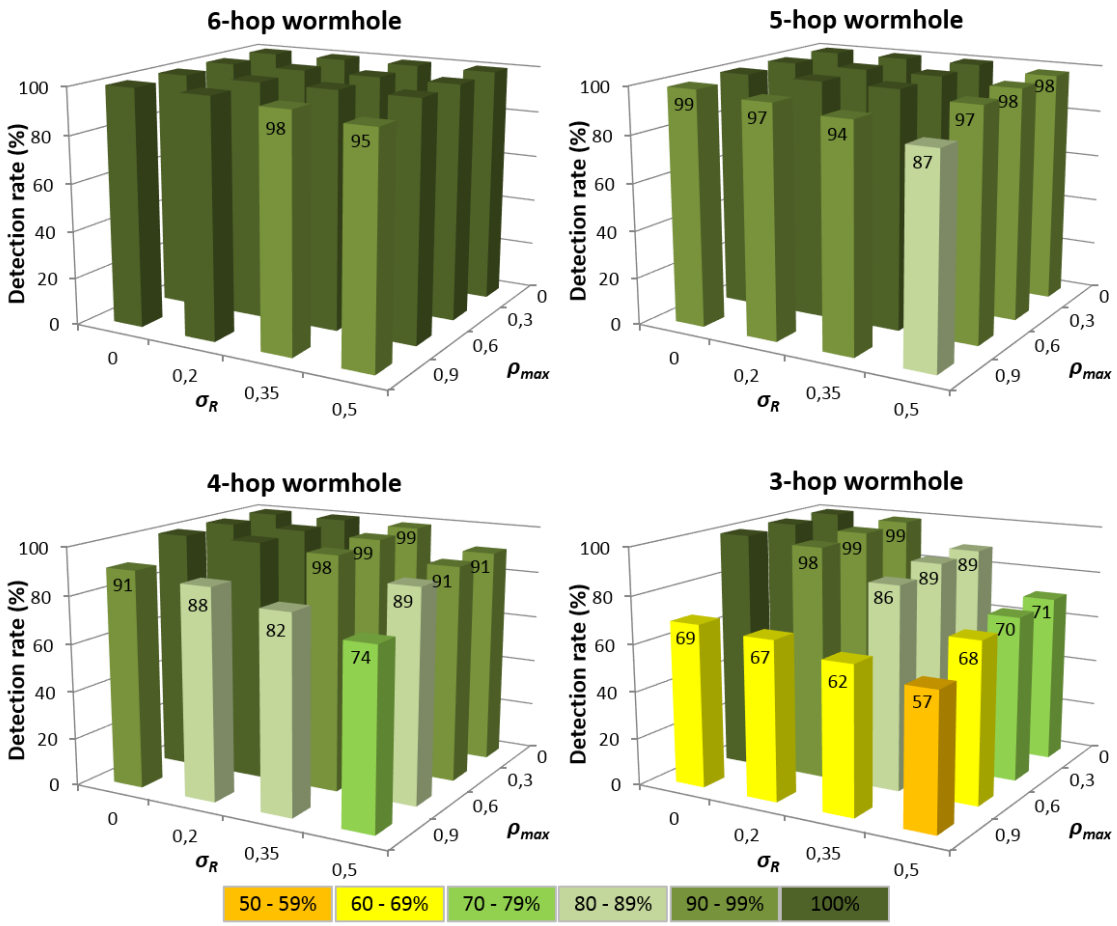

Figure 7.4: Time tampering detection performance for different wormhole lengths, for variable network traffic loads (ρ_{max}), and for variable routing packet service times (σ_R) with at least 15 ΔT_i samples available.

For 3-hop wormholes, the time tampering detection performance drops markedly when there are variations in either network traffic load or routing packet service times, because a healthy node can then often produce a higher ΔT_i than a tampered ΔT_i. This reflects the situation of heavy network traffic loads ($\rho \approx 1$) causing unavoidably long queuing delays and/or high multiprogramming levels leading to increased service times for routing packets. In contrast, the wormhole nodes and those nodes through which routing packets are tunnelled may continue to have negligible loads ($\rho \approx 0$) and correspondingly short packet service times. Despite this decline in performance, tampered ΔT_i values can still be detected with an accuracy of 57% for 3-hop wormholes, when σ_R = 0.5 and ρ_{max} = 0.9. Despite this being lower than the baseline *detection rate* comparator ($\geq$ 70%) defined in Chapter 4, it still represents an important advance to both TTHCA and TTpHA, especially when cognisance

is taken of the stringent criteria necessary to successfully launch a time tampering attack in the first instance.

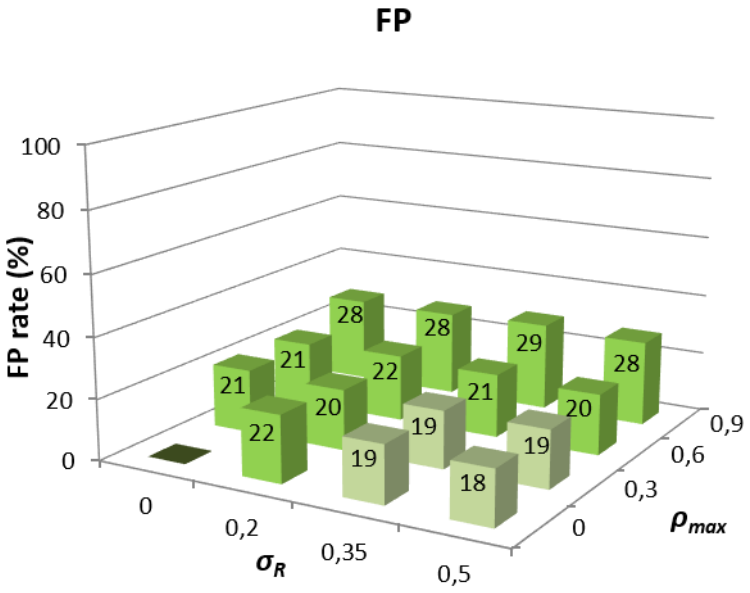

Figure 7.5: FP detection under variable network traffic loads (ρ_{max}) and routing packet service times (σ_R) with at least 15 ΔT_i samples available.

The corresponding *FP rate* remains ≈ 20% for the σ_R range considered, provided $\rho_{max} \leq 0.6$. The reason for this is that the Q-test compares the difference between the two largest ΔT_i values in relation to the difference between $min(\Delta T_i)$ and $max(\Delta T_i)$ which will be approximately constant, regardless of the interval, provided the ΔT_i values are uniformly distributed. When $\rho_{max} = 0.9$, the *FP rate* rises because the queuing delay of a node increases rapidly as ρ tends to 1, and the ΔT_i distributions are no longer uniform. This means a ΔT_i value from a node with high network traffic load can easily become confused with a tampered ΔT_i. Realistically however, even a *FP rate* of ≈30% is still a satisfactory outcome since it fulfils the baseline *FP rate* comparator bound defined in Chapter 4.

7.4.2. CASE 2: MANET Nodes without ΔT_i Track Records

The second set of experiments analysed the situation when a new node joins the MANET and requests a route for the first time. The same conditions are employed as in Section 7.4.1, though now it is assumed *a priori* knowledge is unavailable concerning previously measured

ΔT_i values. The corresponding time tampering detection results are displayed in Figure 7.6. The absence of any track record means that detection performance is not as consistent as CASE 1, though a time tampering *detection rate* of $\geq 80\%$ has still been achieved for all wormhole lengths when $\sigma_R \leq 0.2$ and $\rho_{max} \leq 0.6$. For wormholes ≥ 5 hops, at least 68% of tampered ΔT_i values were correctly detected even when $\sigma_R = 0.5$ and $\rho_{max} = 0.9$, though this is marginally below the baseline comparator level. The equivalent *FP rates*, displayed in Figure 7.7, were slightly higher than in CASE 1 for $\rho_{max} \leq 0.6$ though the baseline comparator was still met under these circumstances. The performance was more sensitive to high network traffic load variations ($\rho_{max} = 0.9$) due to the smaller number of ΔT_i samples. Nevertheless, even a *FP rate* of 45% when $\rho_{max} = 0.9$ does not completely interrupt network communication as more than half of all possible routes are available.

Overall, the time tampering detection performance is less robust in CASE 2 when no ΔT_i track record is available, though this does typify the worst possible MANET situation, when a new node performs its first route discovery procedure. As a node repeatedly runs the route discovery procedure, the corresponding time tampering *detection rate* will quickly improve and converge towards the results presented for CASE 1. This implies that to strengthen the time tampering detection performance for new nodes, it is prudent to run a few route discovery procedures before starting to communicate within the network. This could for instance, be accomplished by specifying within the routing protocol that a node is not allowed to start communicating within a MANET until a minimum of 15 ΔT_i samples have been collected.

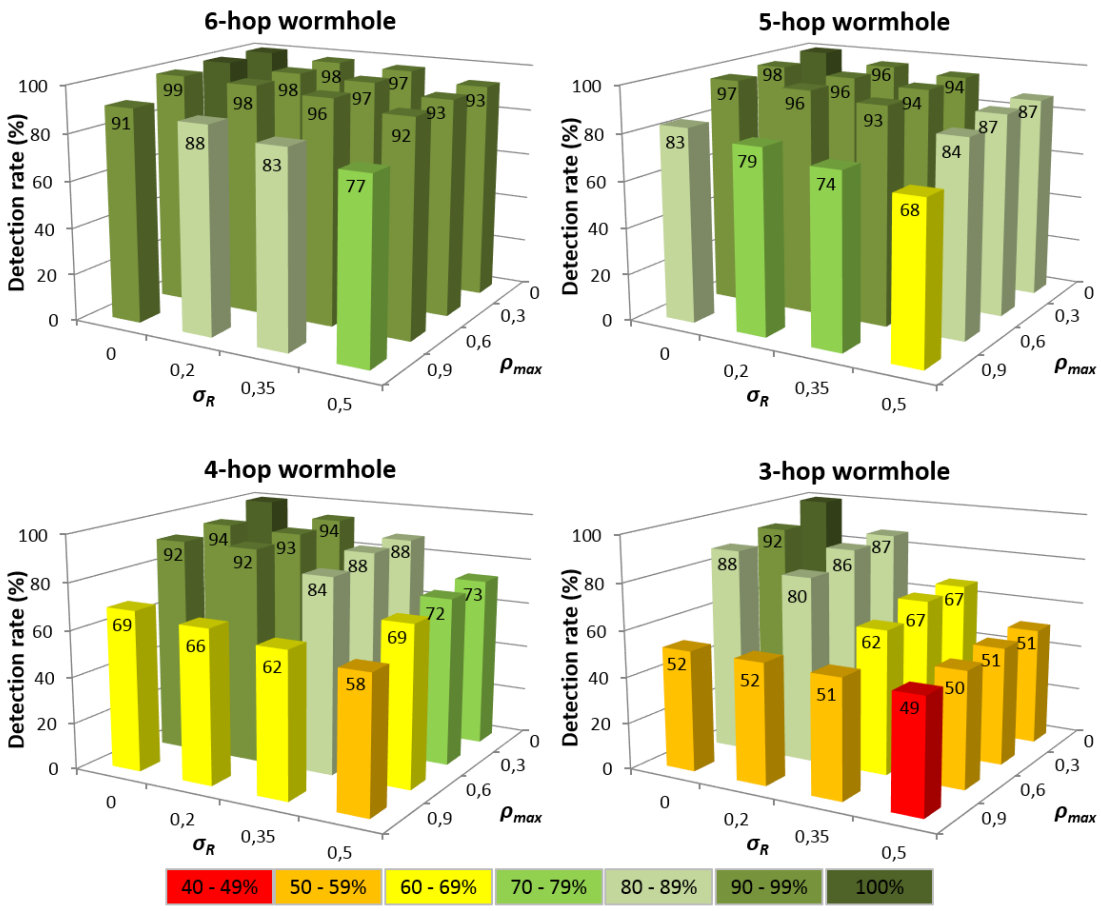

Figure 7.6: Time tampering detection performance for different wormhole lengths under variable network traffic loads (ρ_{max}) and routing packet service times (σ_R) with no available ΔT_i track record.

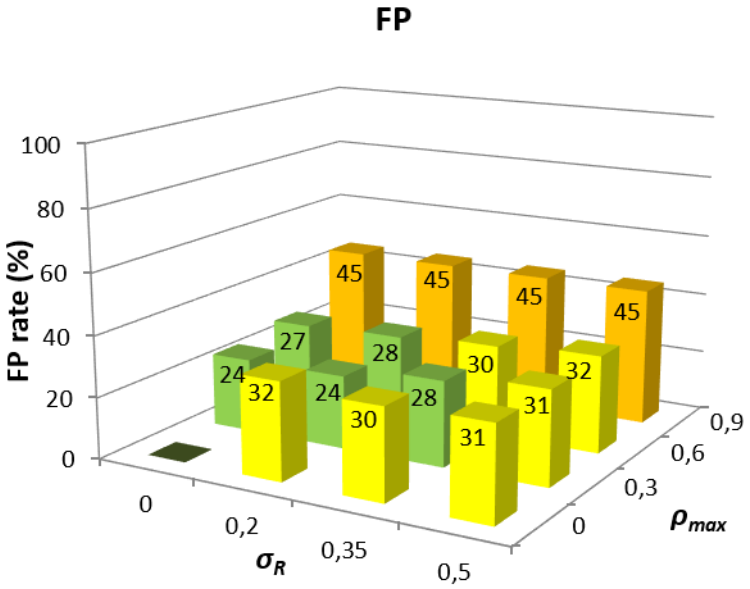

Figure 7.7: False positive detection under variable network traffic loads (ρ_{max}) and routing packet service times (σ_R) with no available ΔT_i track record.

7.4.3. Network Overheads and Computational Complexity

One of the consequences of ΔTVE is a larger $RREP_{TTHCA/TTpHA}$ packet size as it must contain the individual ΔT_i values of each intermediate node of a route, while the original TTHCA and TTpHA mechanism only required the sum ΔT_{TOT}. The size of the ΔT *vector* is dependent on the route HC. If for example each ΔT_i value is represented by 32 bits, then the size of ΔT *vector* at node *#i* will be $32 \cdot HC_i$. This contrasts with the corresponding $RREP_{TTHCA/TTpHA}$ packet which will have a 32 bits ΔT_{TOT} value in each node. A ΔT *vector* with more than one element theoretically increases the transmission and reception time requirements for the routing packet. However, when cognisance is taken of the high bandwidths available in modern wireless technologies, then the extended RREP packets will have negligible performance impact.

The time complexity analysis for the new ΔTVE reveals the only auxiliary cost incurred compared with the original TTHCA and TTpHA algorithms, is the outlier detection scheme performed by the source node, and the only extra operations are those involved in ranking the ΔT *vector* values. Since the number of ΔT *vector* values equals the route HC, the time required for ranking is $O(HC^2)$. However, ranking can be implemented as a linear search of four ΔT values, since the Q-test uses just the three largest and the smallest ΔT *vector* values, so the overall time complexity for ΔTVE is $O(HC)$.

7.4.4. Results Discussion

The desired target in satisfactorily fulfilling research *Objective 3* was to develop a solution that achieved 100% time tampering attack prevention in TTHCA and TTpHA for both I-B and O-B PM wormholes, with no false positive detections and minimal additional network overheads. In critically assessing the performance of ΔTVE, it broadly meets this goal and provides a significant improvement to both TTHCA and TTpHA by detecting a large proportion of time tampering attacks in PM I-B wormholes The results also confirm the

baseline comparator ground truth established in Chapter 4 is largely upheld, with in the majority of test cases, ΔTVE detecting over 70% of time tampering attacks in PM I-B wormholes longer than 4 hops, while the corresponding *FP rate* is < 30%. In shorter wormholes (< 5 hops), the lower ΔT_{F1} and ΔT_{F2} values make it more challenging for ΔTVE to identify time tampering, especially under the conditions of high σ_R and ρ_{max} values. The cost in terms of network overhead is minor since the overall computational complexity is *O(HC)* and the increase of $\text{RREP}_{\text{TTHCA/TTPHA}}$ packets is only $32 \cdot HC_i$ at each node. While there are circumstances where ΔTVE does not always maintain the baseline comparator *detection rates* for I-B wormholes, even the worst-case time tampering *detection rate* is still ≈ 50% which can be viewed as a notable security enhancement to the original TTHCA and TTpHA algorithms taking into account the practical complexities of launching a tampering attack. To fully meet *Objective 3*, further investigations are needed into suitable strategies to both decrease the *FP rate* and improve the accuracy of time tampering detection, especially for PM O-B wormhole links, across the range of σ_R and ρ_{max} values.

7.5. Summary

This Chapter has analysed the conditions for a time tampering attack to succeed in TTHCA and TTpHA from an attacker's point of view and proposed a new security extension called ΔTVE for detecting tampered ΔT_i values in PM I-B wormholes. Simulation results confirmed that ΔTVE provides accurate time tampering attack detection of PM I-B wormholes under a wide range of conditions, though the performance drops to some extent for shorter wormhole links, and when there is high variability in the node packet service times and network traffic loads. Another observation is the relatively high *FP rates* (20% to 45%) which often prevents the shortest route from being used and which can lead to a delay into the route discovery process. Some proposals for addressing these issues allied with new ideas for detecting time tampering in PM O-B wormholes, are presented in a couple of the future framework extensions discussed in the next Chapter.

8. FUTURE DIRECTIONS

8.1. Introduction

The new unified wormhole attack detection framework presented in this thesis makes a series of original contributions to the MANET routing security field. It also affords a rich flexible platform for undertaking further investigations into different aspects of MANET routing security, which extend the findings presented as well as offering new opportunities. Some potential research proposals originating from this work will now be discussed.

8.2. Framework Extensions

TTHCA was introduced as the first step towards a novel wormhole attack detection algorithm based on *packet traversal time* (PTT) analysis. This was followed by an extended version TTpHA which provided greater flexibility and more accurate detection performance under a variety of network conditions. One of the objectives defined for the wormhole detection framework was to be able to detect all wormhole types with low computational overheads, network bandwidth loads and *false positive (FP) rates*. While TTpHA is lightweight in terms of both computational complexity and network bandwidth, it does generate higher *FP rates* under all test conditions, and in particular, a *FP rate* close to 40% when low *timestamp resolution* (TR) wireless hardware is used, i.e. TR = 1 µs. Although this is an insufficiently fine resolution for TTpHA to be relevant in an indoor environment where the radio ranges are typically short, it is still adequate for ensuring good wormhole attack detection performance in outdoor environments with longer ranges. As most current wireless hardware does not have TR < 1 µs, this provides impetus to undertake further investigations into how the *FP rate* can be lowered without impacting on the wormhole *detection rate*. *Lemma 6.1* highlighted the worst case scenario for TTpHA, which is a short route hop count i.e., < 5 hops, since then only a low variability in hop packet traversal time values ($PTT_{i,i+1}$) is permissible for successful wormhole detection. An interesting future

direction for the new framework would be to introduce a minimum length (N_{MIN}) for vector V that must be upheld before the dynamic threshold Θ is calculated by the source node. In practice this would require TTpHA to initially check if the length of $V \geq N_{MIN}$ whenever a source node performs the TTpHA extended AODV route discovery procedure to obtain a route. If this condition is true, then TTpHA proceeds as in Section 6.2.2 to calculate Θ from V. Otherwise, the source node must perform additional route discovery iterations until the length of $V \geq N_{MIN}$. The rationale behind this idea is that by increasing the length of V, the probability of wormhole detection is also increased. Simultaneously, the significance level α, used when calculating Θ from eq. (6.4), can be increased. This has the effect of not only decreasing the false positive level, but because more samples are now available, the wormhole detection performance will still be accurate despite the higher α. The counter argument to introducing N_{MIN} is that there will be higher delays in the route discovery procedure, especially in small networks where the average route hop count is low. Thus, future investigations could focus upon determining the best α and N_{MIN} values to deliver an optimal performance balance for the wormhole detection, false positive occurrence and route delay nexus.

Introducing N_{MIN} and increasing α will not improve *detection rates* for low TR hardware in indoor environments, where radio ranges are short and the $PTT_{i,\ i+1}$ values are small in comparison to the TR. The $PTT_{i,i+1}$ measurement accuracy can however be improved by performing the measurements multiple times, which is a strategy adopted in some *time-of-arrival* (TOA) based indoor positioning systems (Casacuberta & Ramirez, 2012; Wibowo et al., 2009). The drawback with performing multiple PTT measurements during a route discovery procedure is that the latency will be significantly increased and higher network traffic overheads will be incurred. Another interesting research aim would therefore be, to build a real MANET comprising low TR hardware and test the number of $PTT_{i,i+1}$ measurement samples needed to achieve satisfactory wormhole *detection rates*.

8.3. Distributed Time Tampering Detection

A restriction of the new framework is its vulnerability to measurement time tampering. It was revealed in Chapter 7 that while time tampering is very complex to implement from an attacker's point of view and the artificial packet processing time measurement value ΔT_F must be defined within a strict time window in order to succeed, it is still a persistent threat to the wormhole detection performance of both TTHCA and TTpHA. The ΔTVE mechanism introduced for identifying time tampering attacks in TTHCA/TTpHA is based on analysing ΔT_i values. This is only effective on *participation mode* (PM) *in-band* (I-B) wormholes requiring a high ΔT_F value added to the ΔT_i value of a wormhole node, because the delay of the wormhole link is high when packets are tunneled through legitimate nodes. In a PM *out-of-band* (O-B) wormhole, there are no intermediate nodes in the wormhole link so only a small ΔT_F is required and hence ΔTVE cannot discriminate a tampered from a legitimate ΔT_i value. For these reasons, further research is needed to develop more robust strategies to either detect or prevent time tampering attacks in both PM I-B and O-B wormholes.

There also exists considerable potential to explore the application of distributed approaches within the new framework for identifying time tampering in both PM I-B and O-B wormhole detection. By requiring each node in the network to operate in a promiscuous mode, third-party neighbour nodes could potentially be utilized to validate ΔT_i measurements. Consider the MANET scenario in Figure 8.1 where A is the source node, D is the destination node and a route has been established through node B, while the PM O-B wormhole is established between M_1 and M_2. If the third party node C lies within the radio range of both B and M_2, it can eavesdrop upon both the $RREP_{AODV}$ packet delivered to M_2 and also when it is forwarded from M_2 to M1. It can thus measure the time from overhearing reception and the forwarding of this packet. Node C can then compare this time value with the ΔT_i produced

at M_2. If it is smaller than ΔT_i then time tampering is suspected and C can then for instance, broadcast an alert message to its neighbours that M_2 must be omitted from any routing.

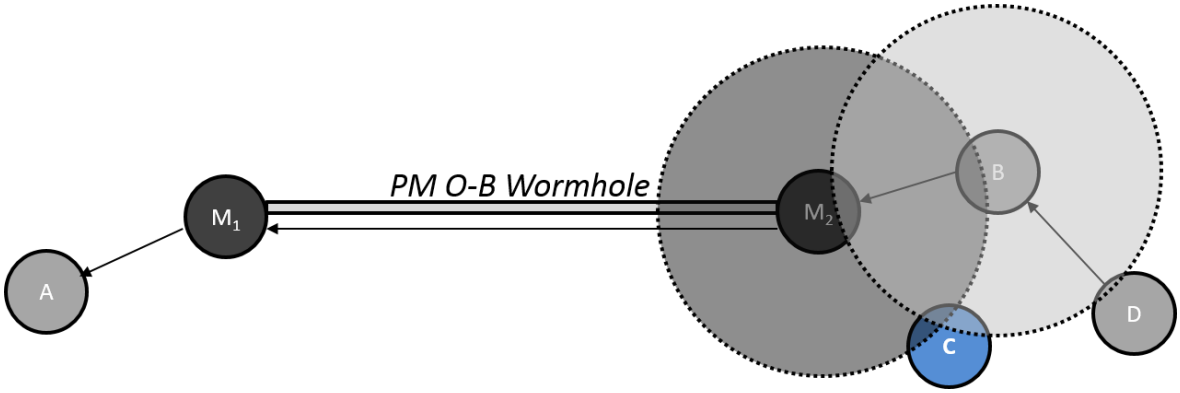

Figure 8.1: A MANET scenario where a third party node C can overhear the reception and forwarding of $RREP_{AODV}$ messages at malicious node M_2 and thus validate the ΔT_i of M_2.

The accuracy of this ΔT_i validation strategy, its corresponding impact upon the network overheads, and the requirements on the node density are all obvious key research questions that need to be critically investigated before consideration can be given to a real world MANET implementation.

8.4. Wormhole Attack Detection using Machine Learning Methods

A broader limitation of current MANET routing security solutions is that several different variants are often needed to provide protection from all threats. For example, the secure routing protocols presented in Chapter 2 typically only provide protection against a subset of threats while either separate algorithms or protocol add-ons are necessary to cover other specific threats, including wormhole attacks. This provides the motivation to explore a single routing security system, such as an IDS, that would offer protection against all known attacks and eliminate the need for using multiple standalone security mechanisms. The use of machine learning based algorithms for MANET IDS is currently an emerging research topic (Nishani & Biba, 2015) since such algorithms offer considerable potential due to their

generic nature. However, current MANET algorithms do not offer full wormhole detection, so the specific features of each wormhole attack type need to firstly be established in order to distinguish between healthy and wormhole infected routes. Some preliminary *proof-of-concept* investigations into this feature engineering process has been presented in Karlsson et al. (2014). A promising future work objective would be to evaluate whether a new wormhole detection model could be trained with reference inputs, based on identifiable features characterising a wormhole link_before being deployed in a real MANET on unknown inputs.

9. CONCLUSION

The self-configuring, infrastructure-less and dynamic topological features of a MANET offer significant implementational and operational advantages including easy and fast large-scale computer network deployments in diverse applications like the IoT, military and extreme emergency environments. However, at the same time they present major challenges relating to QoS provision, connectivity management, end-to-end delay, packet loss on multi-hop routes and IP address management. Security, particularly routing security, is one of the most challenging obstacles to wide scale MANET adoption with wormhole attacks being one of the most severe routing threats. Wormholes are difficult to detect as they can be launched in different modes, with each enforcing its own distinct requirements on the detection mechanism. Many wormhole detection mechanisms have been proposed but most are based on either unrealistic assumptions about the network environment and/or their constituent devices, or exhibit limitations such as they are unable to detect certain wormhole types or are computationally very intensive. This provided the context for the research question addressed in this thesis.

Packet delay analysis based wormhole attack detection schemes have been recognized as easy to implement and low-cost solutions providing the potential to be implemented in a wide range of networks and devices and thus be an attractive viable solution to the research question. Most packet delay analysis based schemes however, are based on *round trip time* (RTT) analysis which is an inaccurate metric for estimating the distance of a route or a hop due to the high variability in node packet processing times.

This thesis has presented a new unified wormhole attack detection framework based on *packet traversal time* (PTT) analysis. This framework is significantly more flexible and accurate compared to existing packet delay based detection mechanisms that use RTT

analysis. It detects all wormhole variants, is adaptive to a range of node hardware and MANET environments, and incurs both low computational and network bandwidth overheads. The framework makes three original scientific contributions to the field of MANET routing security:

i) The most significant innovation is the new wormhole detection algorithm TTpHA that uses a dynamic threshold for the maximum permissible PTT per route hop. TTpHA can tolerate higher radio range fluctuations in node hardware and is more flexible than existing solutions, since it automatically adapts to different network environments. In outdoor environments with long radio ranges, TTpHA can be implemented using low *timestamp resolution* (TR) *off-the-shelf* wireless hardware and tolerates high node mobility during the route discovery procedure, while providing consistently high detection rates. While TTpHA is not yet sufficiently mature to be applied to low TR hardware in indoor environments which inevitably involve short radio ranges, some preliminary future research ideas have been presented to address these challenges.

ii) TTHCA was the first major contribution in the new framework and introduced the novel idea of identifying wormhole attack infected routes based on route PTT analysis. It consistently provided significant improvements in wormhole attack detection performance compared to related RTT-based solutions, while maintaining low network overheads and generating no false positives. Despite encouraging results however, TTHCA was not effective in detecting routes infected by short *participation mode* (PM) *out-of-band* (O-B) wormholes relative to the route hop count (HC). Furthermore, when some of the underlying system assumptions relating to *line-of-sight* (LOS) environments and node hardware were relaxed, high fluctuations in radio ranges led to occurrences of PM O-B wormholes remaining

undetected. The use of a fixed threshold for PTT/HC validation restricted the flexibility of TTHCA to adapt to variable network conditions including, outdoors with long radio ranges and indoors with far shorter ranges. Despite these limitations, TTHCA became a core constituent module within the more advanced TTpHA model in i).

iii) The final contribution is related to how fraudulent packet processing measurements can be successfully identified and prevented in both TTHCA and TTpHA. The prevailing conditions to successfully launch time tampering attacks were firstly analysed and shown to be complicated from an attacker's point of view, since false measurement values had to be defined within a narrow time window. However, they are still feasible and thus considered to be a significant security threat. Time tampering is not only relevant for TTHCA and TTpHA, but equally in other packet delay based wormhole attack detection solutions, such as M-TTM, which involve collaborative time measurements at multiple nodes. A new time tampering detection extension called ΔTVE has been proposed to detect these attacks by applying statistical analysis to collected time measurement values and is the first known time tampering attack detection solution. ΔTVE is consistently able to detect time tampering in PM *in-band* (I-B) wormholes, but PM O-B wormholes are more challenging because their links only need a marginal increase in the time measurement values for an attack to succeed. Some initial ideas for a new distributed approach to detect time tampering in both PM I-B and O-B wormhole detection have been proposed.

In reflecting upon the framework and contrasting with existing state-of-the-art wormhole detection solutions, it offers many innovative features and benefits in terms of wormhole detection, adaptability to diverse MANET scenarios and general low complexity. Practical

issues remain in regard to timestamp resolution of existing hardware especially for indoor environments, and time tampering mechanisms for PM O-B wormholes. Rigorous testing on real MANET devices are also required before the performance and applicability of the presented framework can be fully confirmed. However, as this issue is equivalent for most state-of-the-art wormhole attack detection solutions, due to the lack of real MANET environments, it is cogently contended that the new unified framework is a noteworthy contribution in affording a flexible platform for future real-world wormhole detection solutions in MANET environments.

10. REFERENCES

Azer, M.A., El-Kassas, S.M. & El-Soudani, M.S. (2009) 'Immuning Routing Protocols from the Wormhole Attack in Wireless Ad Hoc Networks', Proceedings of the 4th International Conference on Systems and Networks Communications (ICSNC). Porto, Portugal, 20-25 September. IEEE, pp. 30-36.

Azer, M.A., El-Kassas, S.M. & El-Soudani, M.S. (2010) 'An innovative approach for the wormhole attack detection and prevention in wireless ad hoc networks', Proceedings of the International Conference on Networking, Sensing and Control (ICNSC). Chicago, IL, USA, 11-13 April. IEEE, pp. 366-371.

Barker, K., Wallace, K. & Taylor, M.D. (2015) CompTIA Network N10-006 Cert Guide, Pearson Education.

Basagni, S., Conti, M., Giordano, S. & Stojmenovic, I. (2013) Mobile Ad Hoc networking: The Cutting Edge Directions, 2nd edn, New Jersey, John Wiley & Sons.

Bellavista, P., Cardone, G., Corradi, A. & Foschini, L. (2013) 'Convergence of MANET and WSN in IoT Urban Scenarios', Sensors Journal, vol. 13, no. 10, pp. 3558-3567.

Buchegger, S. & Le Boudec, J. (2002) 'Performance Analysis of the CONFIDANT Protocol', Proceedings of the 3rd International Symposium on Mobile Ad hoc Networking & Computing (MobiHoc). New York, NY, USA, 9-11 June. ACM, pp. 226-236.

Cai, F., Yongquan, C., Lansheng, H. & Zhicun, F. (2013) 'Projection Pursuit Based Wormhole Detection in Ad Hoc Network', Proceedings of the International Conference on Embedded and Ubiquitous Computing (HPCC_EUC). Zhangjiajie, China, 20-25 September. IEEE , pp. 30-36.

Camp, T., Boleng, J. & Davies, V. (2002) ’A Survey of Mobility Models for Ad hoc Network Research’, Wireless Communications and Mobile Computing, vol. 2, no. 5, pp. 483-502.

Casacuberta, I. & Ramirez, A. (2012) ’Time-of-Flight Positioning using the Existing Wireless Local Area Network Infrastructure’, Proceedings of the International Conference on Indoor Positioning and Indoor Navigation (IPIN). Sydney, Australia, 13-15 November. IEEE, pp. 1-8.

Chiu, H. S. & Lui, K-S. (2006) 'DelPHI: Wormhole Detection Mechanism for Ad hoc Wireless Networks', Proceedings of the 1st International Symposium on Wireless Pervasive Computing. Phuket, Thailand, 16-18 January. IEEE, pp. 6-11.

Choi, S., Kim, D-Y., Lee, D-H. & Jung, J-I. (2008) 'WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks', Proceedings of the International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing (SUTC). Taichung, Taiwan, 11-13 June. IEEE, pp. 343-348.

Choudhury, P., Majumder, K. & De, D. (2015) 'Secure and Dynamic IP Address Configuration Scheme in MANET', Advances in Intelligent Systems and Computing, vol. 309, pp. 17-23. [Online]. DOI: 10.1007/978-81-322-2009-1_2 (Accessed 7 December 2015).

Clausen, T., Jacquet, P., Adjih, C., Laouiti, A., Minet, P., Muhlethaler, P., Qayyum, A. & Viennot, L. (2003) 'Optimized Link State Routing Protocol (OLSR)', Request for Comments (RFC) 3626, IETF.

Conti, M. & Giordano, S. (2014) 'Mobile Ad hoc Networking: Milestones, Challenges, and New Research Directions', IEEE Communications Magazine, vol. 52, no. 1, pp. 85-96.

Sourceforge (2015) *Cppcheck - A Tool for Static C/C++ Code Analysis* [Online]. Available at http://cppcheck.sourceforge.net/ (Accessed 20 December 2015).

Dean, R.B. & Dixon, W.J. (1951) ’Simplified Statistics for Small Numbers of Observations’, Analytical Chemistry, vol. 23, no. 4, pp. 636-638.

Dengiz, O., Konak, A. & Smith, A.E. (2011) 'Connectivity Management in Mobile Ad hoc Networks using Particle Swarm Optimization', Ad Hoc Networks, vol. 9, no. 7, pp. 1312-1326.

Dhurandher, S.K., Obaidat, M.S., Verma, K., Gupta, P. & Dhurandher, P. (2011) 'FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems', IEEE Systems Journal, vol. 5, no. 2, pp. 176-188.

Ding, S. (2008) 'A Survey on Integrating MANETs with the Internet: Challenges and Designs', Computer Communications, vol. 31, no. 14, pp. 3537-3551.

Dong, D., Li, M., Liu, Y., Li, X. & Liao, X. (2011) 'Topological Detection on Wormholes in Wireless Ad hoc and Sensor Networks', IEEE/ACM Transactions on Networking, vol. 19, no. 6, pp. 1787-1796.

Dong, D., Liao, X., Liu U., Li, X-Y. & Pang, Z. (2013) 'Fine-Grained Location-Free Planarization in Wireless Sensor Networks', IEEE Transactions on Mobile Computing, vol. 12, no. 5, pp. 971-983.

Eissa, T., Abdul Razak, S., Khokhar, R. & Samian, N. (2013) 'Trust-Based Routing Mechanism in MANET: Design and Implementation', Mobile Networks and Applications, vol. 18, no. 5, pp. 666-677.

Exel, R., Gaderer, G. & Loschmidt, P. (2010) ’Localisation of Wireless LAN Nodes using Accurate TDoA Measurements’, Proceedings of the Wireless Communications and Networking Conference (WCNC). Sydney, Australia, 18-21 April. IEEE, pp. 1-6.

Gao, C. & Jäntti, R. (2004) ’Least-hop Routing Analysis of On-demand Routing Protocols’, Proceedings of the 1st International Symposium on Wireless Communication Systems (ISWCS). Mauritius, 20-22 September. IEEE, pp. 215-219.

García-Otero, M. & Población-Hernández, A. (2012) 'Detection of Wormhole Attacks in Wireless Sensor Networks Using Range-free Localization', Proceedings of the 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD). Barcelona, Spain, 17-19 September. IEEE, pp. 21-25.

Geiger, D.J. (2010) 'High Resolution Time Difference of Arrival Using Timestamps for Localization in 802.11b/g Wireless Networks', Proceedings of the Wireless Communications and Networking Conference (WCNC). Sydney, NSW, Australia, 18-21 April. IEEE, pp. 1-6.

Goldsmith, A. (2005) *Wireless Communications*, Cambridge, Cambridge University Press.

Goyal, P., Batra, S. & Singh, A. (2010) 'A Literature Review of Security Attack in Mobile Ad-hoc Networks', International Journal of Computer Applications, vol. 9, no. 12, pp. 11-15.

Gross, D., Shortle, J.F., Thompson, J.M. & Harris, C.M. (2008) Fundamentals of Queueing Theory, 4th edn, New York, Wiley-Interscience.

Grubbs, F.E. (1969) 'Procedures for Detecting Outlying Observations in Samples', Technometrics, vol. 11, no. 1, pp. 1-21.

Guoxing, L., Zhigang H., Li, L. & Hussain, M.J. (2014) 'Real-time and passive wormhole detection for wireless sensor networks', Proceedings of the 20th International Conference on Parallel and Distributed Systems (ICPADS). Hsinchu, Taiwan, 16-19 December. IEEE, pp. 592-599.

Gupta, A. & Gupta, A.K. (2014) 'A Survey: Detection and Prevention of Wormhole Attack in Wireless Sensor Networks', Global Journal of Computer Science and Technology, vol. 14, no. 1, pp. 22-31.

Gupta, A.K., Sadawarti, H. & Verma, A.K. (2013) 'Performance Analysis of MANET Routing Protocols in Different Mobility Models', International Journal of Information Technology and Computer Science, vol. 5, no. 6, pp. 73-82. [Online]. DOI: 10.5815/ijitcs.2013.06.10 (Accessed 7 December 2015)

Gupta, N. & Khurana, S. (2008) 'SEEEP: Simple and Efficient End-to-End Protocol to Secure Ad Hoc Networks against Wormhole Attacks', Proceedings of the 4th International Conference on Wireless and Mobile Communications (ICWMC). Athens, Greece, 27 July - 1 August. IEEE pp. 13-18.

Haas, Z.J., Pearlman, M.R. & Samar, P. (2002) 'The Zone Routing Protocol (ZRP) for Ad hoc Networks', Internet draft, IETF.

Hongmei, D., Li, W. & Agrawal, D.P. (2002) ’Routing Security in Wireless Ad hoc Networks’, Communications Magazine, vol. 40, no. 10, pp. 70-75.

Hu, Y. (2002) 'Ariadne: A Secure On-demand Routing Protocol for Ad hoc Networks', Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom). Atlanta, GA, USA, 23-28 September. ACM, pp. 12-23.

Hu, Y-C., Johnson, D.B. & Perrig, A. (2002) 'SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks', Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA). Lake District National Park, UK, 2-10 December. IEEE, pp. 3-13.

Hu, Y-C., Perrig, A. & Johnson, D.B. (2003) 'Packet leashes: a Defense against Wormhole Attacks in Wireless Networks', Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM). San-Francisco, CA, USA, 30 March - 3 April. IEEE, pp. 1976-1986.

Jain, S., Tuan T. & Baras, J.S. (2012) 'Wormhole Detection Using Channel Characteristics', Proceedings of the International Conference on Communications (ICC). Ottawa, ON, Canada, 10-15 June. IEEE, pp. 6699-6704.

Jen, S., Laih, C. & Kuo, W. (2009) 'A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET', Sensors, vol. 9, no. 6, pp. 5022-5039.

Johnson, D.B. & Maltz, D.A. (1996) 'Dynamic Source Routing in Ad Hoc Wireless Networks', in Imielinski, T. & Korth, H.F. (eds) Mobile Computing, Springer US, pp. 153-181.

Jones, M.C. & Sibson, R. (1987) 'What is Projection Pursuit?', Journal of the Royal Statistical Society. Series A (General), vol. 150, no. 1, pp. 1-37.

Jøsang, A. (2001) 'A Logic For Uncertain Probabilities', International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 09, no. 03, pp. 279-311.

Karlsson J., Dooley L.S. and Pulkkis, G. (2016) 'A Packet Traversal Time per Hop based Adaptive Wormhole Detection Algorithm for MANETs', Proceedings of the 24th International Conference on Software, Telecommunications and Computer Networks (SoftCOM'16). Split, Croatia, 22-24 September. IEEE, pp. 1–7. **Winner of Best Paper Award**

Karlsson, J., Dooley, L.S. & Pulkkis, G. (2011) 'A New MANET Wormhole Detection Algorithm based on Traversal Time and Hop Count Analysis", Sensors, vol. 11, no. 12, pp. 11122-11140.

Karlsson, J., Dooley, L.S. & Pulkkis, G. (2013) 'Identifying Time Measurement Tampering in the Traversal Time and Hop Count Analysis (TTHCA) Wormhole Detection Algorithm', Sensors, vol. 13, no. 5, pp. 6651-6668.

Karlsson, J., Dooley, S., Laurence & Pulkkis, G. (2012) 'Routing Security in Mobile Ad hoc Networks', Issues in Informing Science and Information Technology, vol. 9, pp. 369-383.

Karlsson, J., Westerlund, M., Dooley, L. & Pulkkis, G. (2014) 'Feature Engineering for Detection of Wormhole Attacking in Mobile Ad Hoc Networks with Machine Learning Methods', Proceedings of the Seminar on Current Topics in Business, Information Technology and Analytics (BITA). Helsinki, Finland, 13 October. Arcada University of Applied Sciences, pp. 3-11.

Khabbazian, M., Mercier, H. & Bhargava, V.K. (2006) 'NIS02-1: Wormhole Attack in Wireless Ad Hoc Networks: Analysis and Countermeasure', Proceedings of the Global Telecommunications Conference (GLOBECOM). San Francisco, CA, USA, 27 November - 1 December. IEEE, pp. 1-6.

Khabbazian, M., Mercier, H. & Bhargava, V.K. (2009) 'Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad hoc Networks', IEEE Transactions on Wireless Communications, vol. 8, no. 2, pp. 736-745.

Khan, Z.A., Rehman, S.U. & Islam, M.H. (2013) 'An Analytical Survey of State of the art Wormhole Detection and Prevention Techniques', International Journal of Science and Engineering REsearch, vol. 4, no. 6, pp. 1723-1731.

Khurana, S. & Gupta, N. (2008) 'FEEPVR: First End-to-End Protocol to Secure Ad Hoc Networks with Variable Ranges against Wormhole Attacks', Proceedings of the 2nd International Conference on Emerging Security Information, Systems and Technologies (SECURWARE). Cap Esterel, France, 25-31 August. IEEE, pp. 74-79.

Koul, A. & Sharma, M. (2015) 'Cumulative Techniques for Overcoming Security Threats in Manets', International Journal of Computer Network and Information Security, vol. 7, no. 5, pp. 61-73.

Krentz, K. & Wunder, G. (2014) '6LoWPAN Security: Avoiding Hidden Wormholes Using Channel Reciprocity', Proceedings of the 4th International Workshop on Trustworthy Embedded Devices (TrustEd). Scottsdale, AR, USA, 3-7 November. ACM, pp. 13-22.

Kurkowski, S., Camp, T. & Colagrosso, M. (2005) ’MANET Simulation Studies: The Current State and New Simulation Tools’, Mobile Computing and Communications Review, vol. 9, no. 4, pp. 50-61.

Lee, G., Seo, J. & Kim, D. (2008) 'An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks', Proceedings of the International Conference on Information Security and Assurance (ISA). Busan, South Korea, 24-26 April. IEEE, pp. 220-225.

Li, S., Xu, L. & Zhao, S. (2014) 'The Internet of Things: A Survey', Information Systems Frontiers, vol. 17, pp. 243-259.

Li, X., Lyu, M.R. & Liu, J. (2004) 'A Trust Model based Routing Protocol for Secure Ad hoc Networks', Proceedings of the IEEE Aerospace Conference. , 6-13 March. IEEE, pp. 1286-1295.

Liang, B. & Haas, Z. J. (1999) ’Predictive Distance-based Mobility Management for PCS Networks’, Proceedings of the 18th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM). 21-25 March. IEEE, pp. 1377-1384.

Lindeberg, M., Kristiansen, S., Plagemann, T. & Goebel, V. (2011) 'Challenges and Techniques for Video Streaming over Mobile Ad hoc Networks', Multimedia Systems, vol. 17, no. 1, pp. 51-82.

Lu, X., Dong, D. & Liao, X. (2013) 'WormPlanar: Topological Planarization Based Wormhole Detection in Wireless Networks', Proceedings of the 42nd International Conference on Parallel Processing (ICPP). Lyon, France, 1-4 October. IEEE, pp. 498-503.

Mahajan, V., Natu, M. & Sethi, A. (2008) 'Analysis of Wormhole Intrusion Attacks in MANETs', Proceedings of the Military Communications Conference (MILCOM). San Diego, CA, USA, 16-19 November. IEEE, pp. 1-7.

Mallapur, S.V. & Patil, S.R. (2012) 'Survey on Simulation Tools for Mobile Ad-Hoc Networks', International Journal of Computer Networks and Wireless Communications (IJCNWC), vol. 2, no. 2, pp. 241-248.

Marwaha, S., Indulska, J. & Portmann, M. (2008) 'Challenges and Recent Advances in QoS Provisioning, Signaling, Routing and MAC protocols for MANETs', Proceedings of the Telecommunication Networks and Applications Conference (ATNAC). Adelaide, SA, Australia, 7-10 December. IEEE, pp. 97-102.

Mashal, I., Alsaryrah, O., Chung, T., Yang, C., Kuo, W. & Agrawal, D.P. (2015) 'Choices for Interaction with Things on Internet and Underlying Issues', Ad Hoc Networks, vol. 28, pp. 68-90.

Mcdonald, J. H. (2014) *Handbook of Biological Statistics*, 3 edn. Baltimore, Sparky House Publishing.

Michiardi, P. & Molva, R. (2002) 'Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks', Proceedings of the IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security. Portoroz, Slovenia, 26-27 September. Kluwer, pp. 107-121.

Microsemi. (2013) IEEE 1588 *Packet Timestamper and Clock and 1Gbps Parallel-to-Serial MII Converter* [Online], Microsemi Corporation. Available at http://www.microsemi.com/document-portal/doc_view/126640-max24288-data-sheet-2013-01 (Accessed 20 December 2015).

Nadeem, A. & Howarth, M.P. (2013) 'A Survey of MANET Intrusion Detection and Prevention Approaches for Network Layer Attacks', IEEE Communications Surveys Tutorials, vol. 15, no. 4, pp. 2027-2045.

Nishani, L. & Biba, M. (2015) 'Machine learning for Intrusion Detection in MANET: A State-of-the-art Survey', Journal of Intelligent Information Systems, pp. 1-17. [Online] DOI: 10.1007/s10844-015-0387-y (Accessed 7 December 2015)

Papadimitratos, P. & Haas, Z. (2002) 'Secure Routing for Mobile Ad Hoc Networks', Mobile Computing and Communications Review, vol. 1, no. 2, pp. 27-31.

Papadimitratos, P. & Haas, Z.J. (2003) 'Secure Link State Routing for Mobile Ad hoc Networks', Proceedings of the Symposium on Applications and the Internet Workshops (SAINT). Orlando, FR, USA, 27-31 January. IEEE, pp. 379-383.

Perkins, C.E. & Bhagwat, P. (1994) 'Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers', Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM). Seattle, WA, USA, 17-22 August. ACM, pp. 234-244.

Perkins, C.E. & Royer, E.M. (1999) 'Ad-hoc on-demand Distance Vector Routing', Proceedings of the 2nd Workshop on Mobile Computing Systems and Applications (WMCSA). New Orleans, LA, USA, 25-26 February. IEEE, pp. 90-100.

Perrig, A., Song, D., Canetti, R., Tygar, J. & Briscoe, B. (2005) 'Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction', Request for Comments (RFC) 4082, IETF.

Qazi, S., Raad, R., Mu, Y. & Susilo, W. (2013) 'Securing DSR against Wormhole Attacks in Multirate Ad hoc Networks', Journal of Network and Computer Applications, vol. 36, no. 2, pp. 582-592.

Qian, L., Song, N. & Li, X. (2005) 'Detecting and Locating Wormhole Attacks in Wreless Ad hoc Networks Through Statistical Analysis of Multi-path', Proceedings of the Wireless Communications and Networking Conference (WCNC). New Orleand, LA, USA, 13-17 March. IEEE, pp. 2106-2111.

Rorabacher, D.B. (1991) 'Statistical Treatment for Rejection of Deviant Values: Critical Values of Dixon's Q Parameter and Related Subrange Ratios at the 95% Confidence Level", Analytical Chemistry, vol. 63, no. 2, pp. 139-146.

Royer, E. M., Mellar-Smith, P. M. & Mosler, L. E. (2001) ’An Analysis of the Optimum Node Density for Ad hoc Mobile Networks’, Proceedings of the IEEE International Conference on Communications (ICC). Helsinki, Finlan, 11-14 June. IEEE, pp. 857-861.

Saha, H.N., Bhattacharyya, D., Bandhyopadhyay, A.K. & Banerjee, P.K. (2012) 'Two-Level Secure Re-routing (TSR) in Mobile Ad Hoc Networks', Proceedings of the International Conference on Advances in Mobile Network, Communication and its Applications (MNCAPPS). Bangalore, India, 1-2 August. IEEE, pp. 119-122.

Samian, N., Maarof, M.A. & Razak, S.A. (2008) 'Towards Identifying Features of Trust in Mobile Ad Hoc Network', Proceedings of the 2nd Asia International Conference on Modeling Simulation (AMS). Kuala Lumpur, Malaysia, 13-15 May. IEEE, pp. 271-276.

Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C. & Belding-Royer, E.M. (2002) 'A secure routing protocol for ad hoc networks', Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP). Paris, France, 12-15 November. IEEE, pp. 78-87.

Sarkar, N.I. & McHaney, R. 2012, 'Modeling and Simulation of IEEE 802.11 Wireless LANs: A Case Study of a Network Simulator', in Al-Bahadili, H. (ed) Simulation in Computer Network Design and Modeling: Use and Analysis, Hershey, IGI Publishing, pp. 85-99.

Shi, F., Liu, W., Jin, D. & Song, J. (2013) 'A Countermeasure against Wormhole Attacks in MANETs using Analytical Hierarchy Process Methodology', Electronic Commerce Research, vol. 13, no. 3, pp. 329-345.

Song, S., Wu, H. & Choi, B-Y. (2012) 'Statistical Wormhole Detection for Mobile Sensor Networks', Proceedings of the Fourth International Conference on Ubiquitous and Future Networks (ICUFN). Phuket, Thailand, 4-6 July. IEEE, pp. 322-327.

Soni, D.M.K., Suri, P.P.K. & Tomar, P. (2010,) 'Article: A Comparative Study for Secure Routing in MANET', International Journal of Computer Applications, vol. 4, no. 5, pp. 17-22.

Su, M. (2010) 'WARP: A Wormhole-avoidance Routing Protocol by Anomaly Detection in Mobile Ad hoc Networks', Computers & Security, vol. 29, no. 2, pp. 208.

Sundararajan, T., Ramesh, S., Maheswar, R. & Deepak, K. (2014) 'Biologically Inspired Artificial Intrusion Detection System for Detecting Wormhole Attack in MANET', Wireless Networks, vol. 20, no. 4, pp. 563-578.

Tran, P.V., Hung, L.X., Lee, Y., Lee, S. & Lee, H. (2007) 'TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks', Proceedings of the 4th Consumer Communications and Networking Conference (CCNC). Las Vegas, NV, USA, 11-13 January 2007. IEEE, pp. 593-598.

Tukey, J.W. (1977) *Exploratory Data Analysis*, Reading, Addison-Wesley.

Vandana, C.P. & Devaraj, F.S. (2013) 'WAD-HLA: Wormhole Attack Detection Using Hop Latency And Adjoining Node Analysis In MANET', International Journal of Engineering Research and Technology, vol. 2, pp. 1-6.

Wang, W. & Bhargava, B. (2004) 'Visualization of Wormholes in Sensor Networks', Proceedings of the 3rd ACM Workshop on Wireless Security (WiSe). Philadelphia, PA, USA, 1 October. ACM, pp. 51-60.

Wang, W., Bhargava, B., Lu, Y. & Wu, X. (2006) 'Defending Against Wormhole Attacks in Mobile Ad hoc Networks: Research Articles', Wireleless Communications & Mobile Computing, vol. 6, no. 4, pp. 483-503.

Verma, S. P. & Quiroz-Ruiz, A. (2006) ’Critical Values for Six Dixon Tests for Outliers in Normal Samples up to Sizes 100, and Applications in Science and Engineering’, Revista Mexicana de Ciencias Geológicas, vol. 23, no. 2, pp. 133-161.

Wibowo, S. G., Klepal M. & Pesh, D. (2009) ’Time of Flight Ranging using Off-the-shelf WiFi Tags’, Proceedings of the International Conference on Positioning and Context-Awareness. 28 May.

Yi, S., Naldurg, P. & Kravets, R. (2001) 'Security-Aware Ad Hoc Routing for Wireless Networks', Proceedings of the 2nd ACM International Symposium on Mobile Ad hoc Networking & Computing (MobiHoc). Long Beach, CA, USA, 4-5 October. ACM, pp. 299-302.

Yovanof, G.S. & Hazapis, G.N. (2009) 'An Architectural Framework and Enabling Wireless Technologies for Digital Cities & Intelligent Urban Environments', Wireless Personal Communications, vol. 49, no. 3, pp. 445-463.

Yu, M., Zhou, M. & Su, W. (2009) 'A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments', IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 449-460.

Zapata, M.G. (2002) 'Secure Ad hoc On-demand Distance Vector Routing', ACM SIGMOBILE Mobile Computing and Communications Review, vol. 6, no. 3, pp. 106-107.

Zhong, X., Tao, Y., Wang, J., Mei, L. & Gu, C. (2015) 'An Investigation on AODV Routing Protocols for MANETs', in Shao, F., Shu, W. & Tian, T. (eds) Information Technology and Career Education, CRC Press, pp. 67-75.

Zhou, J., Cao, J., Zhang, J., Zhang, Z. & Yu, Y. (2012) 'Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Testbed', Proceedings of the 26th International Conference on Advanced Information Networking and Applications (AINA). Fukouka, Japan, 26-29 March. IEEE, pp. 59-56.